SymplyPRO XTL 8 and XTL 24 Gen2 Tape Library User Guide

Thank you for purchasing SymplyPRO XTL

If you have any support questions that are not addressed in this document, then please check our extensive FAQs or submit a support ticket on our support site.

Your feedback is important to us, so please let us know what you think of our products via email hello@gosymply.com





SYMPLY provides this publication “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. SYMPLY may revise this publication from time to time without notice.

IN NO EVENT WILL SYMPLY. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SYMPLY. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING, OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA

Table of Contents

Regulatory Information....9
FCC (United States)....10
Perchlorate warning....10
Prop65 Warning....10
Canadian Verification....10
CE Statement....11
VCCI....11
Recycling and disposal....11
Warnings and Symbols....12
Document Revision....13
About this guide....13
COPYRIGHT STATEMENT....13
Introduction....14
SymplyPRO XTL 8....14
SymplyPRO XTL 24....14
Preparing the host....15
SymplyPRO XTL 8 and XTL 24 Hardware Overview....16
SymplyPRO XTL 8 Part Numbers....16
Physical Specifications SymplyPRO XTL 8....16
SymplyPRO XTL 24 Part Numbers....17
Physical Specifications SymplyPRO XTL 24....17
Environmental Specifications SymplyPRO XTL 8 and XTL 24....18
Transport and Storage of Library and Data Cartridge....18
SymplyPRO XTL 8 and XTL 24 Front View....19
OCP LEDs....20
Operator Control Panel (OCP) Buttons....21
SymplyPRO XTL 8 and XTL 24 Rear View....22
Controller Health Status Indicator....23
LTO Drive Sleds....23
Power Supply LEDs....24
Element Numbering....25
Acclimatization Time for SymplyPRO XTL and Data Cartridge....25
LTO Drive and Data Cartridge Compatibility Guide....26
LTO-9 Media Optimization....26
Installing the SymplyPRO XTL 8 and XTL 24....28

Unpacking the SymplyPRO XTL 8 28
What's in the box XTL 8? 29
Unpacking the SymplyPRO XTL 24 29
What's in the box XTL 24? 30
Location Requirements 31
Removing the shipping lock 32
Shipping Lock Location XTL 8 32
Shipping Lock Location XTL 24 33
Host SAS Configuration Requirements 33
Host Fibre Channel Configuration Requirements 35
iSCSI Configuration Requirements 35
Host iSCSI Host System Requirements 36
Thunderbolt Configuration Requirements 37
Host Thunderbolt Host System Requirements 38
Rack mounting the XTL 8 and XTL 24 39
Required Tools for Rack Mounting 39
To Install the Library in a rack 40
Installing Tape Drives 42
Connecting SAS Cables 43
Connecting Fibre Channel Cables 44
Installing XTL Ethernet Module 44
Installing XTL Thunderbolt Module 46
Powering On the XTL 8 and XTL 24 48
Before power on the SymplyPRO XTL 48
Power on the SymplyPRO XTL 48
Verifying the Host Connection 49
Installing Windows Library and Tape Drivers 49
Verifying the Installation 50
Configuring Additional Features 50
Tape Cartridges and Magazines 51
Using and Maintaining Tape Cartridges 51
Labeling Tape Cartridges 52
Write Protecting Tape Cartridges 53
Read and Write Compatibility 54
Barcode Reader 54
Magazines 54

Inserting tape cartridges into a magazine 55
Mailslots 56
Initial Setup of the Library 57
Different Operating Modes of the SymplyPRO XTL 24 57
Library Interfaces: 57
Using the OCP 58
OCP Default Credentials 58
Using the RMI 59
Remote Management Unit (Web Interface) Credentials 59
Default IP Address 59
Using the Initial Configuration Wizard on the OCP 60
Operating the Library using the Operator Panel 61
OCP Login 62
Magazine States 62
Operations via OCP 62
Magazine Unlock Left 62
Magazine Unlock Right 63
Mailslot Unlock 63
Configuration via OCP 64
Library Configuration 64
Network 64
Users 65
Maintenance via OCP 65
Restore Config from USB 65
Save Log to USB Device 66
Update Firmware from USB Device 66
Save Drive Dump to USB Device 66
Upgrade Drive from USB Device 66
Information/Status in OCP 66
Library Status 67
Network Status 67
Drive 1 Status 68
Drive 2 Status 68
Logout OCP 69
Operating the library using the RMI 70
Using the Library Main Screen on the RMI 70

Top Banner Elements....71
Left Pane Elements....72
Library Status Overview....73
Centre Pane Elements....74
Configuring the Library on the RMI....75
Saving, Restoring and Resetting the Library Configuration....75
Configuring the Date and Time Format....76
Configuring Media Barcode Compatibility Checking....78
License Key Handling....79
Configuring the Library Network Settings....80
Configuring Tape Drives....81
Enabling or Disabling Mailslots....82
Configuring Web Management....83
Configuring Certificate Setting....83
Configuring Network Management....85
Configuring Library Partitions....89
Configuring Encryption....92
Configuring User Accounts....94
Maintaining the Library on the RMI....106
System Test....106
Slot to Slot Test....106
Element to Element Test....108
Position Test....110
Wellness Test....111
Robotic Test....112
Viewing Log Files....112
Downloading Log and Trace Files....113
Managing System Firmware....113
Managing Drive Firmware....114
Downloading Support Tickets....115
Rebooting the Library via RMI....116
Rebooting Drives via RMI....116
Controlling the UID LEDs....117
Operating the Library on the RMI....118
Moving Media via RMI....118
Opening a Magazine via RMI....120

Cleaning a Tape Drive via RMI 120
Rescanning the Cartridge Inventory via RMI 121
Forcing a Drive to Eject a Cartridge via RMI 121
LTO-9 New Media Initialization Wizard 122
Viewing Status Information on the RMI 124
Viewing Library and Module Status 124
Using Inventory Lists 126
Using Inventory Graphical View 128
Using Partition Map Configuration Status 131
Viewing Drive Status 133
Viewing Network Status 134
Viewing Security Status 135
Hardware Servicing of the Library 136
Identifying a Failed Component 137
Replacing a Tape Drive 137
Removing a Tape Drive 138
Removing a Drive Bay Cover 139
Installing a Tape Drive 139
Verifying the Installation 140
Removing and Replacing a XTL Module – Ethernet or Thunderbolt 140
To remove a XTL Module 140
To replace XTL Module 140
Moving the Library 142
To move a library within a rack or into a different rack 143
Replacing a Power Supply 143
Identifying the Failed Component 143
Preparing to Remove the Power Supply 144
Removing the Power Supplies 144
Installing the New Power Supply 144
Verifying the Power Supply Installation and Operation 145
Replacing a Controller Board 146
Identifying the Failed Component 146
Saving the Configuration 146
Powering Off the Library 146
Preparing to Remove the Controller Board 146
Removing the Library Controller 147

Installing the Library Controller 147
Powering On the Library 147
Verifying the Library Controller Installation 148
Removing and replacing the base chassis 149
Remove the existing chassis from the rack 151
Install the replacement chassis in the rack 151
Return the old chassis: 152
Library Troubleshooting 153
Installation problems – Troubleshooting 153
Quick checks (in order) 153
Compatibility 153
Host adapter installation 153
Data-protection application 154
Interface-specific checks 154
OS visibility tests 155
Before contacting support (collect) 155
Performance troubleshooting 156
Average File Size 156
File storage system 156
Connection from the host to disk storage 157
Backup/archive Server 157
Backup/archive software and method 157
Connection from the host to the library 158
Media 158
Operation Problems 159
Power Problems 159
Failure/Attention Indications Displayed on the Front Panel 160
Tape Movement Problems 160
Media Problems 161
Attention LED is Lit 162
Inventory Problems 163
RMI Network Connection Issues 163
Cleaning Problems 164
Finding Event Information 164
Unlocking the Magazine 164
Using the Magazine Unlock Button 164

Using the RMI to Unlock Magazines....165
Using the Manual Release to Unlock Magazines....165
Unloading a Stuck Tape....166
Running Library Tests....166
Acronyms and Abbreviations....167
Event Codes....168
Error Events....168
Warning Events....177
Configuration Change Events....191
Informational Events....193
Warranty Information....196

Regulatory Information

This section describes the tape autoloader compliance with safety and regulatory agency standards.

!	**IMPORTANT**	To comply with the following regulations and standards, the tape autoloader must be properly installed in an office or industrial environment with shielded cables and adequate grounding of the input power.

Device Standards

- ANSI Small Computer System Interface-2 (SCSI-2), X3.131 – 1994
- ANSI SCSI-3 Primary Commands, X3.301 - 1997
- ANSI Information and Technology. SCSI-3 Medium Changer Commands (SMC), NCITS.314:1998
- ANSI SCSI Parallel Interface-2 (SIP-2), X3.302:1998
- IEC 60297 Rack Standards

FCC (United States)

The computer equipment described in this manual generates and uses radio frequency (RF) energy. If the equipment is not installed and operated in strict accordance with the manufacturer's instructions, interference to radio and television reception might result.



Tested To Comply

With FCC Standards

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Part 15, Class A, of the FCC Rules, is designed to provide reasonable protection against radio and television interference in a residential installation. Although the equipment has been tested and found to comply with the allowed RF emission limits, as specified in the above cited Rules, there is no guarantee that interference will not occur in a particular installation. Interference can be determined by turning the equipment off and on while monitoring radio or television reception. The user may be able to eliminate any interference by implementing one or more of the following measures:

- Reorient the affected device and/or its receiving antenna.
- Increase the distance between the affected device and the computer equipment.
- Plug the computer and its peripherals into a different branch circuit from that used by the affected device.
- If necessary, consult an experienced radio/television technician for additional suggestions.

Perchlorate warning

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. www.dtsc.ca.gov/hazardouswaste/perchlorate".

Prop65 Warning

Using this product can expose you to chemicals including lead, which is known to the state of California to cause cancer.

For more information go to www.P65Warnings.ca.gov

Canadian Verification

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations (ICES-003, Class A)

CE Statement

This product conforms to the following European Directive(s) and Standard(s): Application of Council Directives: 73/23/EEC, 89/336/EEC. Standards to which Conformity is declared: EN60950, EN55022, EN55024, EN61000-3-2, EN61000-3-3.

VCCI

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Recycling and disposal

NOTE Disposal of Waste Equipment by Users in Private Household in the European Union and Norway



This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your equipment by handling it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at this time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Warnings and Symbols

IMPORTANT All safety and operating instructions should be read before this product is operated, and should be retained for future reference. This unit has been engineered and manufactured to assure your personal safety. Improper use can result in potential electrical shock or fire hazards. In order not to defeat the safeguards, observe the following basic rules for its installation, use and servicing.



DANGER **High voltage!**

Risk of electric shock.

Do not remove cover (or back). No user-serviceable parts inside. Refer servicing to qualified service personnel.



DANGER A danger condition due to the weight of the unit. Weight symbols are accompanied by an approximation of the product's weight.



CAUTION A discharge of static electricity can damage static-sensitive devices or micro circuitry. Proper packaging and grounding techniques are necessary precautions to prevent damage.



NOTE Provides additional information.

Document Revision

Title: SymplyPRO XTL 8 and XTL 24 Gen2 User Guide

Date: October 23/rd, 2026

Document Version: 1.1

Library Firmware: 1.0.0-B000

About this guide

This guide is intended for system administrators and general users who need physical and functional knowledge of the SymplyPRO XTL 8 1U Autoloader and SymplyPRO XTL 24 2U Library.

This guide provides information about:

- Installing the Gen 2 SymplyPRO XTL 8 Autoloader and SymplyPRO XTL 24 2U Library
- Configuring and operating the SymplyPRO XTL 8 Autoloader and SymplyPRO XTL 24 2U Library
- Troubleshooting the Gen 2 SymplyPRO XTL 8 Autoloader and SymplyPRO XTL 24 2U Library
- Upgrading and servicing the Gen 2 SymplyPRO XTL 8 Autoloader and SymplyPRO XTL 24 2U Library
- Installing the Optional Remote Management Unit (RMU).
- Installing the Gen 2 SymplyPRO XTL 8 Autoloader and SymplyPRO XTL 24 2U Library in a rack.

COPYRIGHT STATEMENT

© 2026 SYMPLY. All rights reserved.

Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of SYMPLY is prohibited. SymplyPRO is a trademark in the U.S. and other countries. All other trademarks are the property of their respective companies.

LTO and Ultrium are trademarks of HP, IBM, and Quantum in the U.S. and other countries. All other trademarks are the property of their respective companies.

Introduction

SymplyPRO XTL 8

The SymplyPRO XTL 8 Gen 2 Tape Autoloader provides a compact, high-capacity, low-cost solution for simple, unattended data backups and archives. This unique design houses up to **8** tape cartridges in a compact 1U form factor with easy access to tape cartridges via two removable magazines and a mail slot. The magazines can hold up to **4** (left magazine including **mailslot**) cartridges.

The SymplyPRO XTL 8 Gen 2 Tape Autoloader can support **one half-height** LTO tape drives either **SAS** or **Fibre Channel (FC)**. The autoloader occupies one SCSI target address and uses dual LUNs for the tape drive and autoloader robotic. The SymplyPRO XTL 8 Tape Autoloader can operate via Operator Control Panel (OCP) or via the Remote Management Unit (RMU).

SymplyPRO XTL 8 Gen 2 is compatible with most operating systems that support SAS or FC. To leverage advanced library features, use an operating system with a compatible medium-changer driver or a **supported backup/archive application**.

SymplyPRO XTL 24

SymplyPRO XTL 24 Gen 2 is a compact, automated LTO tape library designed for simple, high-capacity backup and archive workflows. In a 2U form factor it houses up to **24** cartridges via two front-accessible, removable magazines (left magazine with **mailslot** and right magazine), each holding up to **12** cartridges for fast media handling.

The library supports **one or two LTO half-height** tape drives with **SAS** or **Fibre Channel (FC)** connectivity. Devices are presented using **multiple LUNs** so that the tape drive(s) and the library robotics are visible to the host separately.

Optional connectivity modules extend deployment flexibility:

- **SymplyPRO XTL Ethernet Module** — dual **10 GbE (iSCSI)** bridging for SAS-attached drives. In the XTL 24, the module occupies the **top drive bay**, so the library supports **one** LTO drive when installed.
- **SymplyPRO XTL Thunderbolt Module** — dual **Thunderbolt 3** (one host, one daisy-chain) for direct attachment. In the XTL 24, the module also occupies the **top drive bay**, so the library supports **one** LTO drive when installed.

SymplyPRO XTL 24 Gen 2 is compatible with most operating systems that support SAS or FC. To leverage advanced library features (robotics, barcodes, partitioning, etc.), use an operating system with a compatible medium-changer driver or a **supported backup/archive application**.

Preparing the host

For the best experience in using the SymplyPRO XTL 8 and XTL 24 it is important to make sure that the host server or workstation is correctly configured.

Symply recommend you follow these general guidelines:

- To get optimum performance from your SymplyPRO XTL a SAS or Fibre Channel HBA is required in the host that can transfer data at a rate that supports the autoloader's maximum burst transfer speed.
- Make sure that your data protection application supports the SAS or Fibre Channel (FC) HBA installed in the host.
- Install a suitable HBA that supports LUN scanning and TLR.
- Depending on the server configuration, you may need to change the SCSI IDs of the autoloader.
- When the host server is powered on, install the software and/or driver(s) that are compatible with the autoloader. Data protection software packages may require additional software or licensing to communicate with the autoloader robotics.
- Confirm the host server's operating system recognized the autoloader.

For more information on verifying the connections consult the HBA and operating system documentation.

!	**IMPORTANT**	Some host adapters that are also RAID controllers do not support tape libraries. It is important that the host adapters support TLR.

	**TIP**	Symply recommend ATTO SAS and Fibre Channel Host Adapters, they are available from Symply and our authorized resellers.

SymplyPRO XTL 8 and XTL 24 Hardware Overview

SymplyPRO XTL 8 Part Numbers

Part Numbers	Drive Generation	Host Interface	Maximum Native Capacity	Maximum Native Data Transfer
SYXTL-C08S1L8H2-BT	LTO-8	2 x 6Gb SAS SFF-8088	96T B	300MB/Sec
SYXTL-C08S2L9H2-BT	LTO-9	2 x 12Gb SAS SFF-8644	144 TB	300MB/Sec
SYXTL-C08F1L8H2-BT	LTO-8	2 x 8Gb FC LC	96 TB	300MB/Sec
SYXTL-C08F1L9H2-BT	LTO-9	2 x 8Gb FC LC	144 TB	300MB/Sec

Physical Specifications SymplyPRO XTL 8

Characteristic	Description
Rack requirements	Standard 19-inch rack with 1U of clearance
Number of Slots	8
Number of Mailslots	1
Drive Form Factor	Half-Height
Number of Drives	1
Drive Interface	SAS or Fibre Channel
MSBF w/o drive	500,000 hours
Dimensions (H x W x D)	45.6 x 444.5 x 789.5 mm (1.79 x 17.5 x 31.08 in)
Power Supply	Single 80W Module (110 to 240v)
Weight Without Media	11.4 Kg (25.13 lb)
Weight With Media (8 pieces)	13.1 Kg (28.66 lb)
Clearance Rear	Minimum of 154 mm (6.06 in)
Clearance Front	Minimum of 308 mm (12.12 in) – for mailslot Minimum of 600 mm (23.62 in)– for remove magazines
Clearance Side	Minimum of 50.8 mm (2 in)

SymplyPRO XTL 24 Part Numbers

Part Numbers	Drive Generation	Host Interface	Maximum Native Capacity	Maximum Native Data Transfer
SYXTL-C24S1L8H2-BT	LTO-8	2 x 6Gb SAS SFF-8088	288 TB	300MB/Sec
SYXTL-C24S2L9H2-BT	LTO-9	2 x 12Gb SAS SFF-8644	432 TB	300MB/Sec
SYXTL-C24F1L8H2-BT	LTO-8	2 x 8Gb FC LC	288 TB	300MB/Sec
SYXTL-C24F1L9H2-BT	LTO-9	2 x 8Gb FC LC	432 TB	300MB/Sec

Physical Specifications SymplyPRO XTL 24

Characteristic	Description
Rack requirements	Standard 19-inch rack with 2U of clearance
Number of Slots	24
Number of Mailslots	1
Drive Form Factor	Half-Height
Number of Drives	1 or 2
Native Drive Interface	SAS or Fibre Channel
MSBF w/o drive	500,000 hours
Dimensions (H x W x D)	87 x 448 x 740 mm (3.43 × 17.64 × 29.13 in)
Clearance Front	308 mm (2.13 in) for mail slot access 600 mm (23.62 in) for magazine removal
Clearance Rear	154 mm (6.06 in)
Clearance Side	51 mm (2.01 in)
Power Supply	Single Module 160W (AC power 110v – 240v)
Weight Without Media	Single Drive 14.7 Kg (32.41 lbs) Dual Drive 15.6 Kg (34.39 lbs)
Weight With Media	Single Drive 20.2 Kg (44.53 lbs) Dual Drive 21.1 Kg (46.52 lbs)

Environmental Specifications SymplyPRO XTL 8 and XTL 24

Environmental Factor	Recommended	Allowable	Non-Operating
Dry-Bulb Temperature	**LTO-9** and **LTO-10**: 15 to 25 °C (59 to 77 °F) **LTO-7** and **LTO-8**: 16 to 25 °C (61 to 77 °F)	**LTO-9** and **LTO-10**: 15 to 30 °C (59 to 86 °F) **LTO-7** and **LTO-8**: 16 to 30 °C (61 to 86 °F)	5 to 35˚C (41 to 95˚F)
Relative Humidity	**LTO-9** and **LTO-10**: 20 to 50% (non-condensing) **LTO-7** and **LTO-8**: 20 to 50% (non-condensing)	**LTO-9** and **LTO-10**: 20 to 50% (non-condensing) **LTO-7** and **LTO-8**: 20 to 50% (non-condensing)	20 to 80% (non-condensing)
Maximum Temperature Change	5 °C (41°F) / hour	5 °C (41°F) / hour	5 °C (41°F) / hour
Maximum Humidity Change	5% / hour	5% / hour	5% / hour
Temperature Limitation for Humidity Conditions	**LTO-9** and **LTO-10**: Max Dew Point 22 °C (72 °F) **LTO-7** and **LTO-8** Wet Bulb Temperature <= 26 °C (79 °F)		
Maximum Altitude	3,048 m (10,000 ft)	3,048 m (10,000 ft)	12,192 m (40,000 ft)
Dust concentration	Less than 200 microgram / cubic metre		

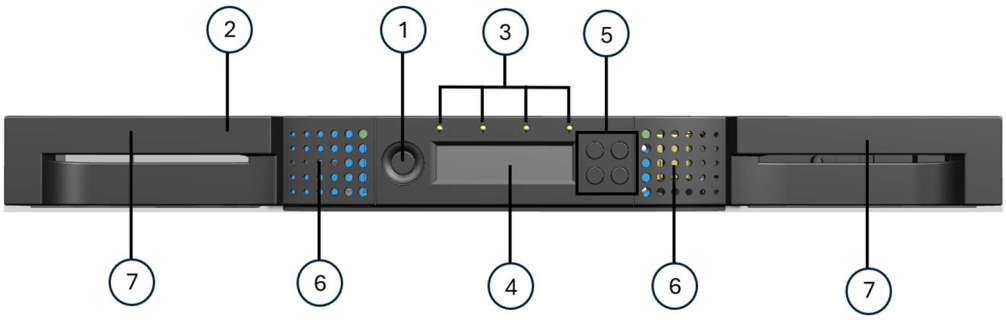
Transport and Storage of Library and Data Cartridge

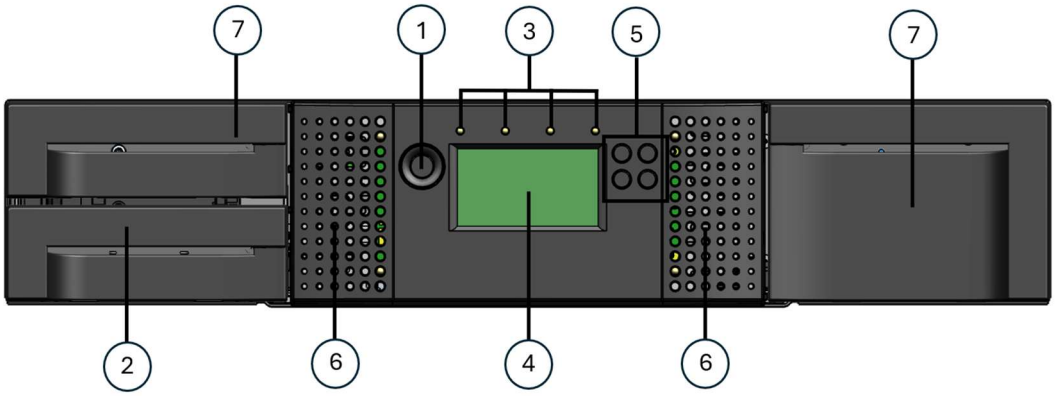
Condition	Environmental Specification
Short-term Storage condition	See operating conditions
Long-term Storage condition	See operating conditions
Shipping Conditions	5 to 45 °C (41 to 113 °F); 10% to 80% non-condensing. RH; 26 °C (72 °F) dew point maximum

!	**IMPORTANT**	Data cartridges stored at a temperature in excess of 52°C (125.6 °F) may suffer permanent damage. It is important that both temperature and humidity should be kept constant, as rapid changes in either are not good for the data cartridges or LTO drives.

SymplyPRO XTL 8 and XTL 24 Front View

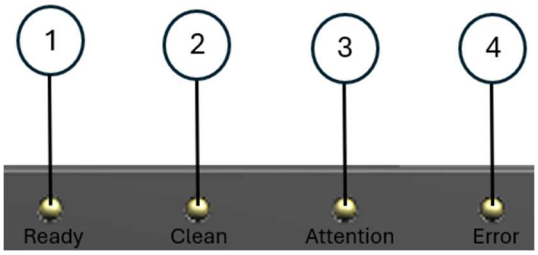
The front of the SymplyPRO XTL 8 is used to access the power button, Operator Control Panel (OCP), left and right magazines, LED's, and the mail slot.





Number	Description
1	Power Button
2	Left Hand Side Magazine (inc Mailslot)
3	Front Panel LED
4	Front Panel LCD
5	Control Buttons
6	Air Vents
7	Right Hand Side Magazine

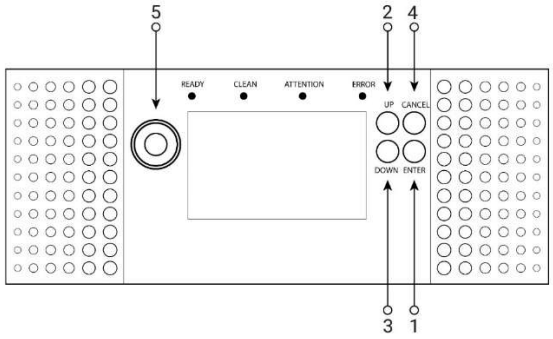
OCP LEDs



Number	LED	Colour	Description
1	Ready / Activity	Green	Illuminated when power is on. Blinking when there is tape or autoloader robotics activity.
2	Clean Drive	Amber	Illuminated when the tape drive has determined that a cleaning cartridge should be used. Cleaning is only necessary when the autoloader directs you to do so. Additional cleaning is not necessary. The LED will be turned off after the tape drive is cleaned successfully.
3	Attention	Amber	Illuminated if the autoloader has detected a condition that requires attention by the operator. Media might be bad, marginal or invalid. It will be cleared when all invalid cartridges have been exported from the tape autoloader.
4	Error	Amber	Illuminated if an unrecoverable tape drive or autoloader error occurs. A corresponding error message displays on the LCD screen (see for more information). It will be cleared when the error state is resolved.

Operator Control Panel (OCP) Buttons

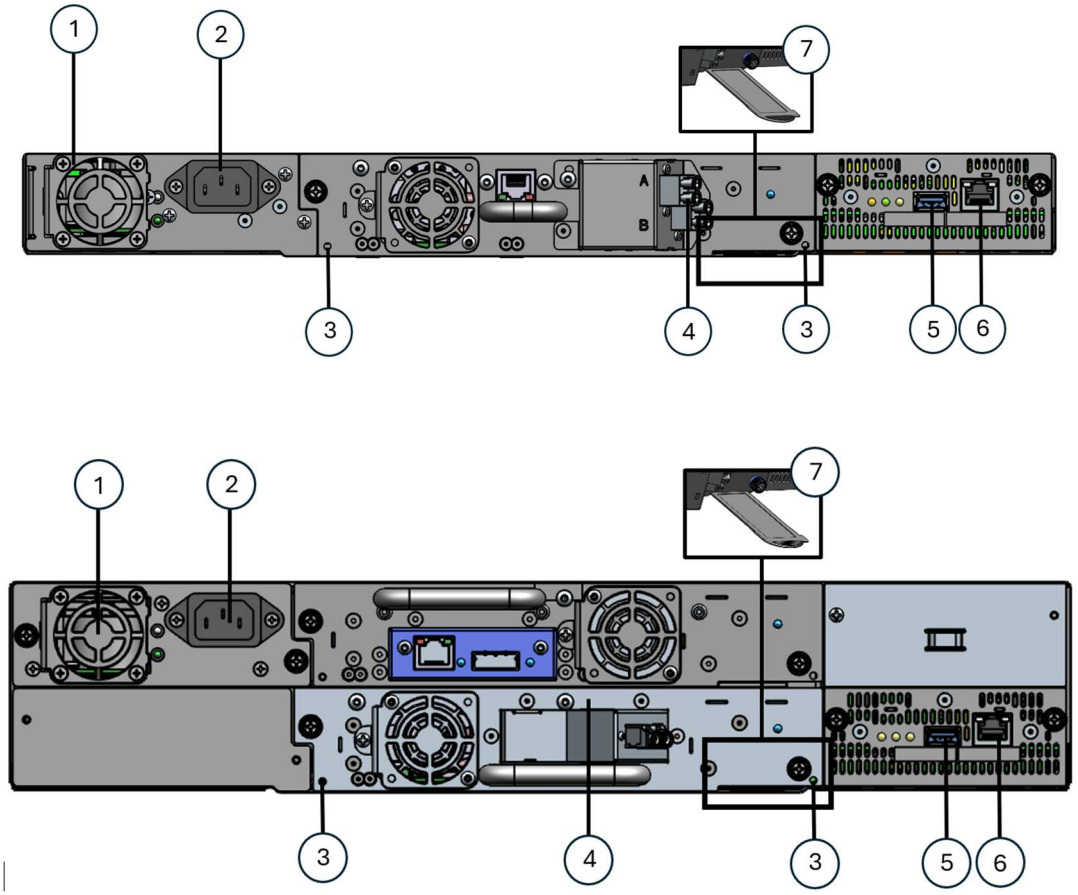
The Operator Control Panel (OCP) consists of an LCD display, 4 push button switches, a power on/off button, and 4 status LEDs. The OCP screen displays actions and status information, menu items or error messages equivalent to the operation mode.



Number	Button	Description
1	Enter Button [↵]	The ENTER button to go to a sub menu or execute an action
2	Up Button [↑]	The UP button is used to navigate through menu items
3	Down Button [↓]	The DOWN button is used to navigate backward through menu item
4	Cancel Button [x]	The CANCEL button is used to cancel a user action and return to the last menu item
5	Power Button	Pressing the POWER ON/OFF button will initiate a controlled Power Down of the unit (soft power down)

SymplyPRO XTL 8 and XTL 24 Rear View

The rear of the tape autoloader provides access to SAS or Fibre Channel (FC) connectors, tape drive bays, the power connector, Ethernet, serial and the USB port.

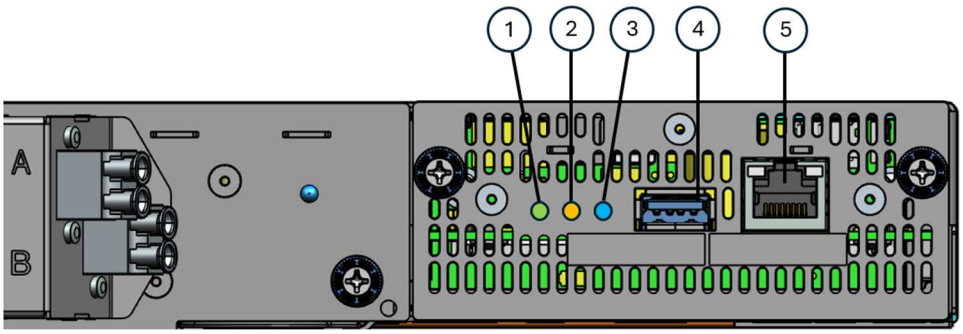


Number	Description
1	Fan
2	Power connector requires 110/220-volt AC power connection.
3	Emergency Magazine Release
4	Tape Drive Sled
5	USB Port
6	Ethernet Management Port
7	Pull-out tab containing the serial number and other product information

NOTE XTL-24 power supply is a customer replaceable unit (CRU). The XTL-8 power supply is not a CRU.

Controller Health Status Indicator

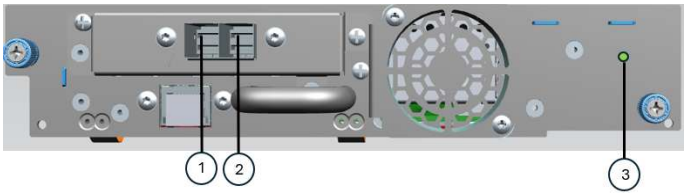
The controller health status indicator are three LEDs. The LEDs are located on the back panel in the middle of the left side.



Number	Colour	Description
1	Green	Controller health status LED. • Pulses on and off in approximately one second cycles during normal operation. • Solid green or not illuminated while the autoloader is powered on indicates that the controller is not operating correctly. • Before replacing the controller, power cycle the autoloader, confirm that the controller is faulty.
2	Amber	Error
3	Blue	Unit identifier (UID)
4	n/a	USB Port
5	n/a	Ethernet Port

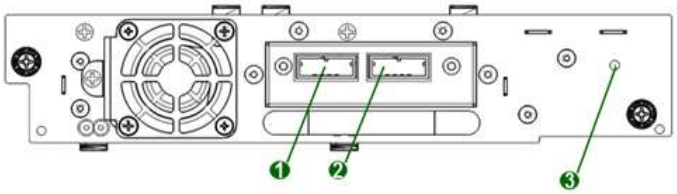
LTO Drive Sleds

LTO-9 Half-Height SAS Dual Port



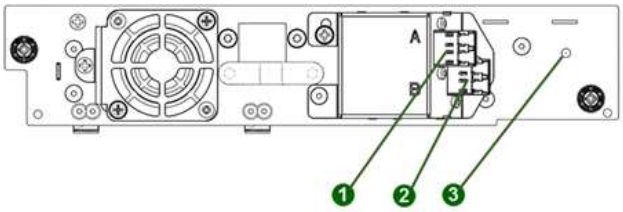
Number	Description
1	Port A (Connect this port)
2	Port B
3	Tape Drive Power LED, Green

LTO-7 & 8 Half-Height SAS Dual Port



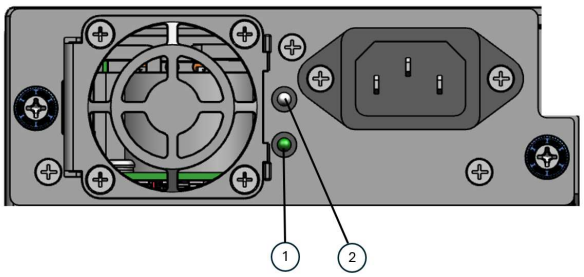
Number	Description
1	Port A (Connect this port)
2	Port B
3	Tape Drive Power LED, Green

LTO Half-Height Fibre Channel Dual Port



Number	Description
1	Port A (Connect this port)
2	Port B
3	Tape Drive Power LED, Green

Power Supply LEDs



Number	Colour	Description
1	Green	Module Powered On
2	White	AC power connected, but Module Powered Off

Element Numbering

The SympyPRO XTL 8 and XTL 24 will generally display logical element numbering of modules, storage slots and tape drives starting with number one from the bottom up.

Logical Numbers (Log ID)

Left Magazine Front	Rear	Library	Right Magazine Front	Rear
1.1 1.2 1.3 1.4		1	1.5 1.6 1.7 1.8	
1.3 1.2 1.1	1.6 1.5 1.4	1	1.15 1.14 1.13	1.18 1.17 1.16
1.9 1.8 1.7	1.12 1.11 1.10		1.21 1.20 1.19	1.24 1.23 1.22

Physical Numbers (PNUM)

Left Magazine Front	Rear	Library	Right Magazine Front	Rear
1 2 3 4		1	5 6 7 8	
3 2 1	6 5 4	1	15 14 13	18 17 16
9 8 7	12 11 10		21 20 19	24 23 22

SCSI Element Address

Left Magazine Front	Rear	Library	Right Magazine Front	Rear
1001 1002 1003 1004		1	1005 1006 1007 1008	
1003 1002 1001	1006 1005 1004	1	1015 1014 1013	1018 1017 1016
1009 1008 1007	1012 1011 1010		1021 1020 1019	1024 1023 1022

Acclimatization Time for SymplyPRO XTL and Data Cartridge

Acclimatisation is required if the SymplyPRO XTL has been stored or transported at a different temperature to the operating environment. As a baseline, allow **four hours** after unpacking for the library to reach ambient temperature.

If there is **no risk of condensation** (i.e., the air is dry and the unit is above the local dew point), you may bring the unit up to temperature more quickly by **powering it on for ~30 minutes** before use. Do **not** load tapes until the unit has stabilised.

If the SymplyPRO XTL is **hotter than the maximum operating temperature (30 °C / 86 °F)**, there is a risk that tape may adhere to the read/write head. In this case, allow the library and drives to **cool back within the operating range** before use.

For best results, store the SymplyPRO product **and** its LTO data cartridges **together for 24 hours** in the environment where they will be used. This helps temperature and humidity equalise, ensuring proper acclimatisation.

LTO Drive and Data Cartridge Compatibility Guide

	LTO-5 Data Cartridge	LTO-6 Data Cartridge	LTO-7 Data Cartridge	LTO-8 Data Cartridge	LTO-9 Data Cartridge	LTO-10 Data Cartridge
SymplyPRO LTO-7	Read Only	Read & Write	Read & Write	n/a	n/a	n/a
SymplyPRO LTO-8	n/a	n/a	Read & Write	Read & Write	n/a	n/a
SymplyPRO LTO-9	n/a	n/a	n/a	Read & Write	Read & Write	n/a
SymplyPRO LTO-10	n/a	n/a	n/a	n/a	n/a	Read & Write

LTO-9 Media Optimization

Overview. LTO-9 media optimisation—also referred to as *characterization*—was introduced with LTO-9 drives and LTO-9 cartridges. Because LTO-9 writes many more, narrower tracks, the drive performs a one-time, per-cartridge calibration to establish a reference that its intelligent alignment system uses to optimise data placement. This improves write reliability and long-term media durability. (Not required when using LTO-8 media in an LTO-9 drive.)

Key points

- **Automatic on first load.** Optimisation runs the first time an LTO-9 cartridge is initialised in any LTO-9 drive.
- **One time per cartridge.** Once completed, the cartridge can be used in any compatible drive without repeating optimisation.
- **Typical duration.** Expect ~**40 minutes** on average. Most complete within **60 minutes**; some may take up to **2 hours**.
- **No impact from duration variance.** The time taken has no effect on cartridge performance or functionality.
- **Do not interrupt.** Let the process complete before starting backup or archive jobs.
- **Pre-optimised media from Symply.** All LTO-9 media included in-box with Symply LTO-9 products ships **pre-optimised**.
- **Available through resellers.** Symply-supplied LTO-9 media is available **with or without** pre-optimisation via our authorised reseller network.



TIP

If you're introducing non-pre-optimised media into a new environment, consider pre-loading cartridges during a maintenance window so optimisation completes ahead of scheduled jobs [Using the LTO-9 New Media Initialization (Optimization) Wizard]

Installing the SymplyPRO XTL 8 and XTL 24

Before you begin

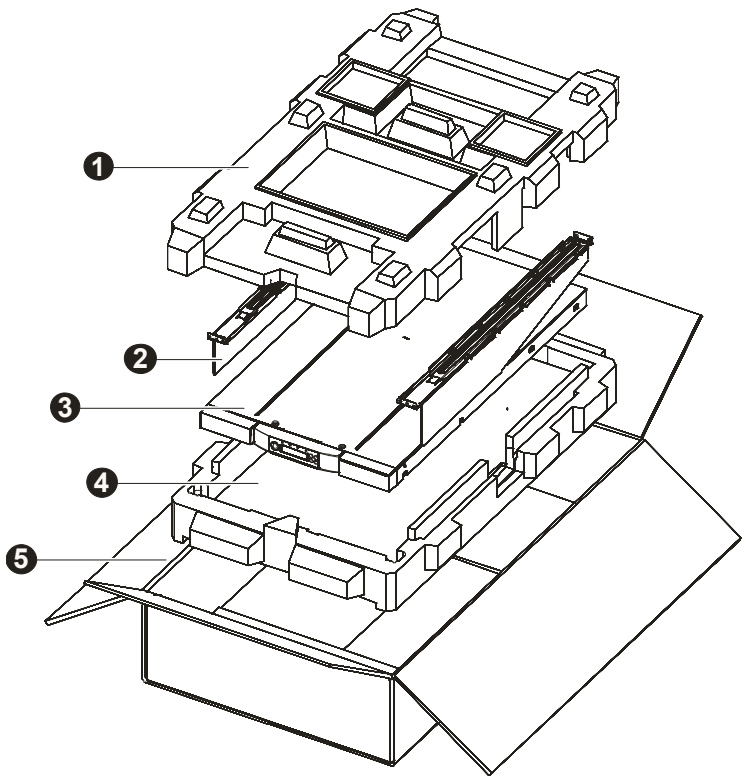
- Inspect the **outer carton** for visible damage.

  If damage is found **do not unbox or install**. Photograph the carton and contents, keep all packaging, and contact your reseller/place of purchase immediately.

Unpacking the SymplyPRO XTL 8

Caution should be used whenever lifting the SymplyPRO XTL in and out of the shipping carton, make sure that the working area around you is free from obstructions.

- Carefully unpack the SymplyPRO XTL.
- Remove the shipping materials from the top of the autoloader.
- Remove the two rack rails and set aside.
- **Carefully lift the autoloader out** of the carton, **remove the bag** from the autoloader.
- **Save the packaging materials** for future use.
- Check contents (see What's in the box).



Number	Description
1	Top Packing Shell
2	Rack rails
3	Autoloader
4	Bottom Packing Shell
5	Shipping Carton

What's in the box XTL 8?

Item	QTY	Description
SymplyPRO XTL 8	1	1U 8 Slot Autoloader with Single Fixed PSU
Rack Kit	1	▪ 2 rack mount rails. ▪ 2 mounting brackets. ▪ 6 x M3 torx screws to fix the mounting brackets (9.5mm square holes) ▪ 6 x M3 torx screws to fix the mounting brackets (9.5mm round holes) ▪ M5 screws to secure the mounting brackets to the rack.
LTO Clean Cartridge	1	SymplyLTO Media - Ultrium Universal Cleaning Cartridge, with barcode
Ethernet Cable	1	Ethernet Cable (for management port)
Data Cable Optical	1	FC Units Only – 1 x 3m OM4 LC-LC Optical Cable
Data Cable SAS	1	SAS Units Only – 1 x 2m SAS Cable ▪ LTO-7 & LTO-8 include SFF-8080 -to- SFF-8644 ▪ LTO-9 include SFF-8644 -to- SFF-8644
Power Cable	1	2 m (6.5 ft) IEC power cord for local region
Welcome Card	1	Information Card Please Read Carefully
Shipping Carton	1	Please retain shipping carton and packaging for warranty purposes

Unpacking the SymplyPRO XTL 24

- Open the carton and **carefully remove the two rack rails**; set them aside with the mounting hardware.
- Remove the **top packing materials**. Take out the accessory kit and set aside.
- With two people, lift the library vertically out of the carton.
- Remove the **protective bag** from the library and the rear foam cushion, then place the unit on a stable surface.
- Visually check the chassis for dents, cracks, or loose parts.
- **Save all packaging materials** for future transport or service.
- Check contents (see What's in the box).

What's in the box XTL 24?

Item	QTY	Description
SymplyPRO XTL 24	1	2U 24 Slot Library with Single PSU
Rack Kit	1	▪ 2 rack mount rails. ▪ 2 mounting brackets. ▪ 6 x M3 Torx screws to fix the mounting brackets (9.5mm square holes) ▪ 6 x M3 Torx screws to fix the mounting brackets (9.5mm round holes) ▪ M5 screws to secure the mounting brackets to the rack.
LTO Clean Cartridge	1	Symply LTO Media - Ultrium Universal Cleaning Cartridge, with barcode
Ethernet Cable	1	3m (9.8 ft) Cat6 Ethernet Cable (for management port)
Data Cable Optical	2	**FC Units Only** – 2 x 3m (9.8 ft) OM4 LC-LC Optical Cable
Data Cable SAS	2	**SAS Units Only** – 2 x 2m (6.5ft) SAS Cable ▪ LTO-7 & LTO-8 include SFF-8088 -to- SFF-8644 ▪ LTO-9 & 10 include SFF-8644 -to- SFF-8644
Power Cable	1	2 m (6.5 ft) IEC power cord for local region
Welcome Card	1	Information Card Please Read Carefully
Shipping Carton	1	Please retain shipping carton and packaging for warranty purposes

Location Requirements

- The XTL 8 and XTL 24 are designed for rack installation only.
- Rack installations must use the provided rack rails.
- Select a location with access to the host server.
- Choose a location that meets the criteria in the table below.

Criteria	Definition
Rack Requirements	Standard 19-inch rack (minimum depth of 800 mm / 31.49 in) with an appropriate # of U's (Rack Units) of clearance for the planned module quantity.
Rack Space Requirements	• 1U for XTL 8 • 2U for XTL 24
Room Temperature	Allowable: 10 - 30 ºC (50 - 86 ºF)
	Recommended: 10 - 25 ºC (50 - 77 ºF)
Power Source	• AC Power Voltage: 100-240 VAC • Line Frequency: 50-60 Hz • Library Located near AC Outlet(s) The AC power cord is the library's main AC disconnect device and must always be easily accessible.
Air Quality	• Place the library in an area with minimal sources of particulate contamination. • Avoid areas near frequently used doors and walkways, stacks of supplies that collect dust, printers, and smoke-filled rooms. • Excessive dust and debris can damage tapes and tape drive. • Less than 200 microgram / cubic metre.
Humidity	Recommended: 20 - 50% RH non-condensing
	Allowable: 20 - 80% RH non-condensing

! IMPORTANT	Connect the library only to a mains outlet with a **protective earth (PE)** and in accordance with **local electrical codes**. **Do not** defeat or remove the earth/ground pin. Improper grounding can cause electric shock, equipment damage, or fire.

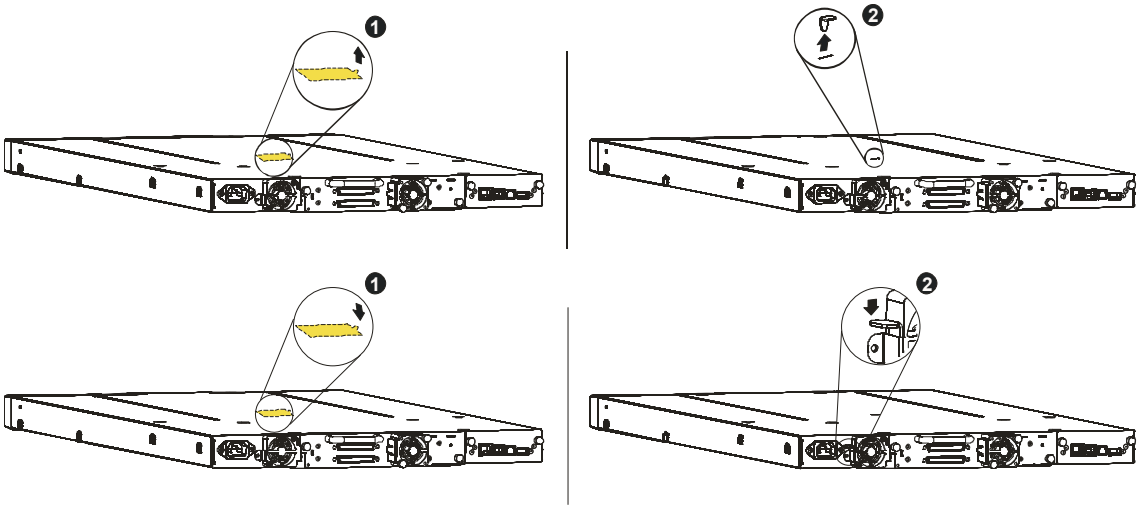
 **CAUTION**	If installing in a rack, **do not exceed** the power capability of the rack PDU(s) or the branch circuit. Consider startup/inrush current and leave reasonable headroom.

Removing the shipping lock

- **Location**: The shipping lock is at the **top centre** of the library, held in place by a **yellow label** marked for removal.
- **Removal**: Gently peel off the yellow label securing the lock to the top panel, then **lift out the lock.**
- After the shipping lock is removed, it should be **stored** for future use.
    - XTL 8: **next to the power supply.**
    - XTL 24: **on the rear panel** right side of the library
- Always reinstall the shipping lock before shipping the library.

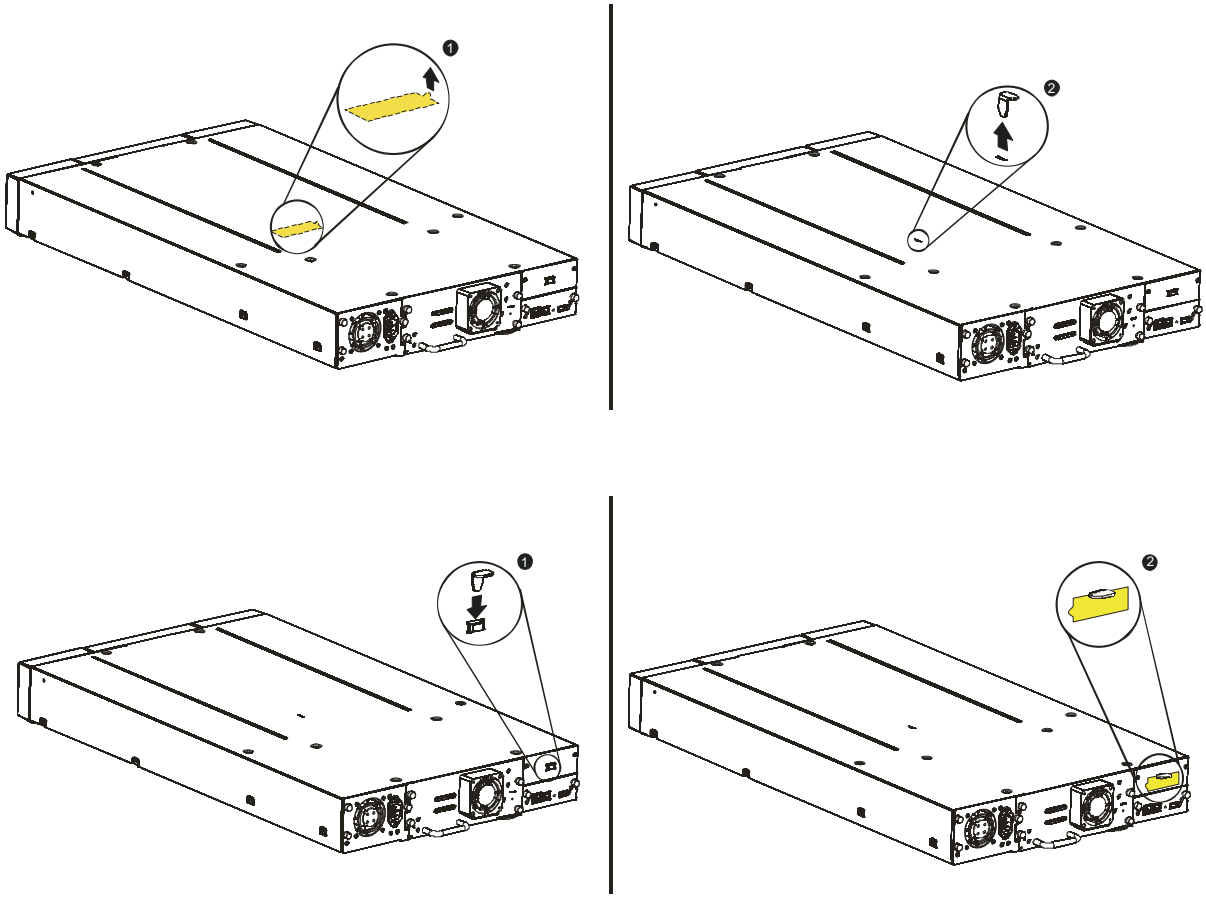
!	**IMPORTANT**	The shipping lock, which prevents the robotic transport mechanism from moving during shipment, must now be removed before the autoloader or library is powered on

Shipping Lock Location XTL 8



!	**IMPORTANT**	The shipping lock, which prevents the robotic transport mechanism from moving during shipment, must now be removed before the autoloader is powered on

Shipping Lock Location XTL 24



!	**IMPORTANT**	The shipping lock, which prevents the robotic transport mechanism from moving during shipment, must now be removed before the autoloader is powered on

Host SAS Configuration Requirements

Serial Attached SCSI (SAS) is a point-to-point storage interface used for devices such as LTO tape drives and libraries. Because SAS links are direct connections rather than a shared parallel bus, you don't have to configure traditional SCSI bus IDs; however, the SCSI protocol (and **LUNs**) still apply over SAS.

Requirements and notes

- **Use a true SAS HBA (not a RAID controller).** Fit a host bus adapter with **external** SAS ports that supports **multiple LUNs** and **LUN scanning** so the OS can discover both the tape drive **and** the library robotics. Many RAID controllers do not expose devices correctly for tape.
- **LUN layout.** SymplyPRO XTL presents a single target per drive with **dual LUNs**: **LUN 0 = tape drive**, **LUN 1 = library robotics**.
- **Lane/port capacity.** A typical external SAS port is a **x4 wide** link (four lanes). An LTO tape drive uses **one lane**, so a single HBA port can service **up to four drives** when cabled appropriately (e.g., via a 1→4 breakout or SAS expander). If you connect one

drive with a single end-to-end cable, only **one lane** is used, and the remaining lanes are idle.

- **Cabling.** Use certified external mini-SAS / mini-SAS HD cables that match the HBA and device connectors. Keep within the HBA's supported cable length and generation (6/12/24 Gb SAS).

TIP	For best results, use an IT-mode/initiator-class SAS HBA, enable **LUN scanning**, and verify in the OS that both a **Tape drive** and a **Medium changer** device is present before configuring your backup application.

Supported speeds by drive generation are shown in the table below:

LTO Generation	Supported Speeds
LTO-7	1.5 Gbps, 3 Gbps, 6 Gbps
LTO-8	1.5 Gbps, 3 Gbps, 6 Gbps
LTO-9	3 Gbps, 6 Gbps, 12 Gbps
LTO-10	3 Gbps, 6 Gbps, 12 Gbps

CAUTION	Always use a high-quality SAS cable. The library has one or more SAS connectors on each SAS tape drive. SAS connectors are keyed. Do not force a SAS cable's SAS connector into the tape drive as it might be keyed differently.

- **Unique identifier.** Each SAS tape drive is identified by a **World Wide Name** (WWN, also called **WWID**). In SymplyPRO XTL, the library assigns the WWID to the **drive bay**, so if a drive is replaced the **same WWID is reassigned** to the new drive in that bay.
- **OS tracking per channel.** The operating system associates the drive's WWID with the **specific HBA channel** it was discovered on. With a fan-out (breakout) cable, each connector corresponds to a separate HBA channel.
- **Keep channel placement stable.** After initial discovery, keep each drive on the **same fan-out leg/channel** to preserve the OS association (WWID ↔ HBA channel). Moving a drive to a different channel can cause the OS or backup software to treat it as a **new device**, potentially requiring reconfiguration.

TIP	Label the fan-out connectors (e.g., A/B/C/D) and match them to drive bay numbers to maintain consistent cabling and predictable device paths.

Host Fibre Channel Configuration Requirements

The Fibre Channel (FC) tape drive can be connected directly to the server with a Host Bus Adapter (HBA) or through a storage area network (SAN).

The installation requires one Fibre Channel cable for each tape drive. The tape drives all utilize an LC-style connector. Some drives will have two FC ports, but only one cable connection is needed per drive. The cable should always be connected to Port A.

Supported speeds by drive generation are listed in the table below:

LTO Generation	Supported Speeds
LTO-7	2 Gbps, 4 Gbps, 8 Gbps
LTO-8	2 Gbps, 4 Gbps, 8 Gbps
LTO-9	2 Gbps, 4 Gbps, 8 Gbps
LTO-10 FH	8 Gbps, 16 Gbs, 32 Gbs

iSCSI Configuration Requirements

10 GbE iSCSI connectivity on **SymplyPRO XTL-24** is enabled by adding the **SymplyPRO XTL Ethernet Module** (dual 10 GbE). The module bridges attached **SAS LTO tape drive** to the IP network as iSCSI targets.

How it works (initiator/target):

- The **host** runs an iSCSI **initiator** (software driver) that sends SCSI commands over IP.
- The **SymplyPRO XTL Ethernet Module** exposes one or more iSCSI **targets** (the bridge to the SAS LTO drives in the library).
- Each initiator and target have a globally unique **iSCSI name** (an **IQN**).

Requirements:

- **Network interface:** A 10 GbE NIC on the host, cabled to the same network/VLAN as the XTL Ethernet Module.
- **iSCSI initiator/driver:**
    - **Windows:** Built-in Microsoft iSCSI Initiator.
    - **Linux:** Native initiator available (e.g., open-iscsi).
    - **macOS:** No built-in initiator; third-party software is required (ATTO Xtend SAN).
- **Multiple LUN support:** Ensure the initiator and applications support **multiple LUNs** so both the **tape drive** and the **library robotics** are discovered.
- **Target discovery:** Configure target portal(s), discover/log in to the **SymplyPRO XTL Ethernet Module** targets, and confirm sessions are established.

- The Ethernet Module presents the LTO drives behind it as iSCSI targets (with LUNs). In line with SymplyPRO Ethernet behaviour, LUN 0 is the **tape drive** and LUN 1 is the **library robotics**—your initiator must enumerate both.
- Each XTL Ethernet Module occupies one LTO drive bay and can bridge **up to four SAS tape drives** per module.



TIP

For stable device paths, use a dedicated iSCSI network (or VLAN), enable initiator auto-reconnect, and verify in the OS that you see both a Tape drive and a Medium changer before configuring your backup application.



NOTE

The SymplyPRO Ethernet module has two data ports. If both data ports are connected to the same host NIC and/or the same switch fabric, place **each data port in a different IP subnet.** Do **not** assign both data ports to the same subnet.

The management port of the SymplyPRO Ethernet module must be on a separate subnet from the data ports.

Host iSCSI Host System Requirements

Windows OS:

- A Windows host computer with a 10GbE NIC with current drivers to support OS version.
- The data ports of the SymplyPRO Ethernet configured to the same network as the 10GbE NIC.
- Microsoft iSCSI Initiator.

Linux OS:

- A Linux host computer with a 10GbE NIC with current drivers to support OS version.
- The data ports of the SymplyPRO Ethernet configured to the same network as the 10GbE NIC.
- An iSCSI Initiator.

macOS:

- A mac host computer with a 10GbE NIC with current drivers to support OS version.
- The data ports of the SymplyPRO Ethernet configured to the same network as the 10GbE NIC.
- macOS version 10.15 or later.
- A macOS compatible iSCSI initiator (ATTO Xtend SAN is approved).

NOTE	The SymplyPRO XTL Ethernet Module requires a minimum 10Gb Ethernet connectivity to the host or the switch.

Thunderbolt Configuration Requirements

SymplyPRO XTL-40 supports Thunderbolt via the **SymplyPRO XTL Thunderbolt 3 Module**, which bridges the library's SAS LTO drives to a host computer over Thunderbolt.

About Thunderbolt. Thunderbolt is a high-speed I/O interface co-developed by Intel and Apple that can carry data, video and power over a single connector. In this application, it's used **solely for data** between the XTL library and the host.

Ports & cables.

- **Thunderbolt 3/4/5** ports use the **USB-C** connector and are identified by the **Thunderbolt lightning-bolt icon** (do not confuse with plain USB-C).
- All SymplyPRO Thunderbolt Modules ship with a **premium 2 m active Thunderbolt 4 cable**, compatible with **Thunderbolt 3 and Thunderbolt 5** host ports.
- Use certified Thunderbolt cables, not generic USB-C cables.
- Connect directly to a host Thunderbolt port (avoid USB-C hubs/docks unless Thunderbolt-certified and qualified for your workflow).
- Ensure your backup/archive software supports tape drives and medium changers connected over Thunderbolt.

NOTE

USB-C Ports that are only USB will not have the lightning bolt icon and are not compatible with Thunderbolt devices.

Thunderbolt 2 Host will require a Thunderbolt 3 (USB-C) to Thunderbolt 2 Adapter.

NOTE

If cable lengths of over 2m are required Symply also supplies Corning Thunderbolt 3 Optical cables which are available in 5, 10-, 15-, 25- and 50-meters lengths.

Host Thunderbolt Host System Requirements

macOS:

- A mac host computer with Thunderbolt 3, 4 or 5 connectivity.
- macOS 11 and later.

Windows OS:

- Windows Hardware with Intel Certified Thunderbolt 3, 4 or 5 connectivity.
- Microsoft Windows 11 and 10.

Windows Server 2022, 2019, and 2016.

Rack mounting the XTL 8 and XTL 24

The SymplyPRO XTL 8 and XTL 24 Gen2 products are easy to install in racks compliant to the EIA 310A Standard, when at least 1000 mm (39.37 in) deep.

WARNING	**Product Weight:** • SymplyPRO XTL 8 weighs 11.4 Kg (25.13 lbs) without media. • SymplyPRO XTL 24 weighs 15.6 Kg (34.39 lbs) without media. **Risk of Personal Injury:** Before moving or lifting a module: • **Observe local health and safety requirements** and guidelines for manual material handling. • Remove all tapes to reduce the weight and to prevent cartridges from falling into the robotics path and damaging the library. • Remove all tape drives to reduce the weight. • Obtain adequate assistance to lift and stabilize the module during installation or removal. **Risk of damage to devices:** When placing a module into or removing the module from a rack: • Extend the rack's levelling jacks to the floor. • Ensure that the full weight of the rack rests on the levelling jacks. • Install stabilizing feet on the rack. • Extend only one rack component at a time.

Required Tools for Rack Mounting

- #3 Phillips screwdriver
- T10 Torx screwdriver

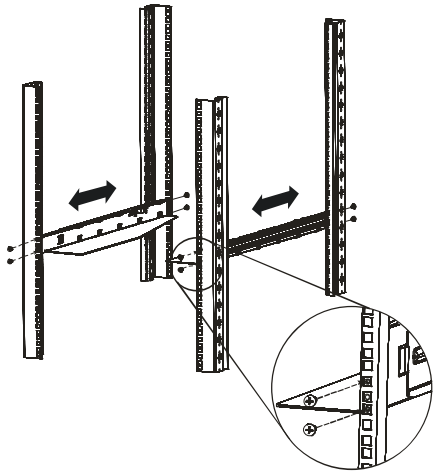
There are two sets of eight M6 screws in the accessory package that came with the autoloader. The type of rack that you have will determine the type of M6 screw that you will use.

 **WARNING**	Risk of personal injury or damage to the autoloader due to the weight! Always remove all tapes to reduce the overall weight of the autoloader. Always observe local health and safety requirements and guidelines for manual material handling.

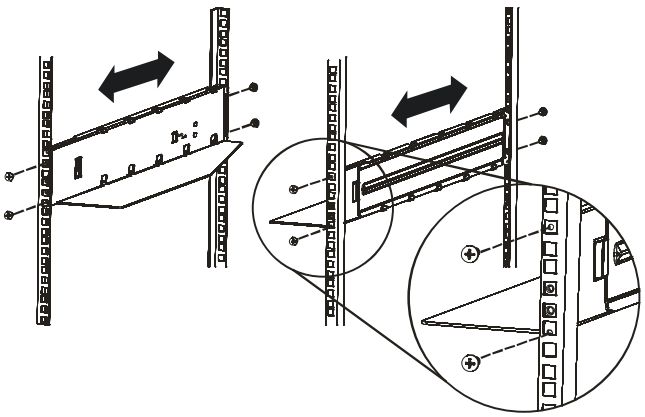
To Install the Library in a rack

1) Unpack the rack kit and verify that it includes the following
    a. Two rails
    b. Packet containing M6 screws
2) Install the rails
    a. Using the screws from the packet for your rack and a #3 Phillips screwdriver, secure the front of one rail to the front of the rack. The support platform of each rail is tapered, narrowing towards the rear.
    b. Extend the rail to the depth of the rack and secure the rail to the back of the rack.
    c. Install the other rail

XTL 8 rails



XTL 24 rails



3) Install the XTL 8 or XTL 24 in the rack
    a. Slide the Library onto the rails.
    b. From the front of the Library, secure the front bezel to the rack using a #2 Phillips screwdriver placed through the small holes in the mounting bracket.
    c. Tighten the captive screws on each side of the Library until they are seated.



4) Verify that the XTL 8 or XTL 24 is contained within the 1U or 2U rack, is level and does not have any weight on the top of the units.

Installing Tape Drives

Skip this step if the drive(s) are already factory installed.

1) **Locate the vacant drive bay** at the rear of the library.
2) **Remove the bay faceplate and cover**.
    a. Unscrew the faceplate screws and lift off the faceplate.
    b. Remove **one** drive-bay cover for the bay you're populating; retain all screws/covers for future use.
3) **Insert the drive**.
    a. Hold the tape drive by the handle, supporting it from underneath.
    b. Slide it along the **alignment rails** until the drive is **flush** with the back of the library (do not force).
4) **Secure the drive**
    a. Finger-tighten the blue captive thumbscrews evenly to fix the drive to the chassis.
    b. If the thumbscrews do not start, back the drive out slightly, re-align on the rails, and try again—**do not use tools** to overtighten.

 **CAUTION**	• If resistance is felt before the drive is flush, re-check that the correct bay cover has been removed and the drive is properly on the rails. • All drive bays without tape drives installed must have drive bay covers installed.

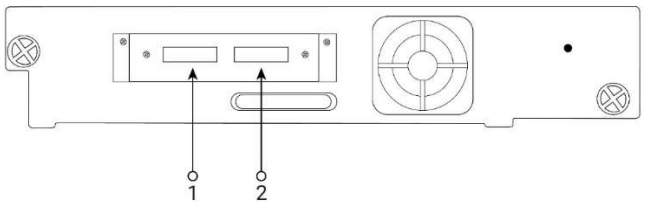


MECHANICAL HAZARD

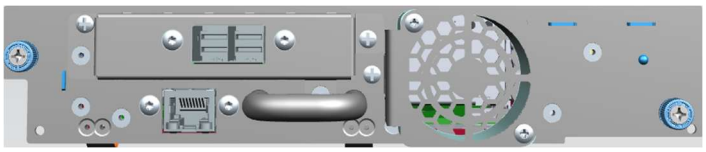
Danger: Risk of hand pinching. Can trap hands, fingers and cause serious injury. Keep hands clear during operation.

Connecting SAS Cables

LTO-7 and LTO-8 SAS drive sled



LTO-9 and LTO-10 SAS drive sled



Number	Description
1	**Port A** – Connect this port only
2	Port B

1) **Connect to the HBA**.
    a. Insert the **HBA end** of the SAS cable into the HBA port until the latch clicks.
    b. **If using a SAS fan-out (1→4) cable:** the **single connector** goes into the **HBA**.
2) **Connect to the drive(s).**
    a. **Single-to-single cable:** attach the other end to the tape drive SAS **port A**.
    b. **SAS fan-out cable:** attach **one x1 leg per tape drive (port A)**—do not daisy-chain. The **unused fan-out legs are single-channel** and **not suitable for disk arrays**. Either use them for additional tape drives on the same HBA port or **coil and secure** them to the rack to avoid strain on connectors.

TIP

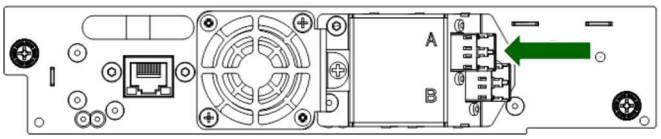
Route and dress cables to avoid sharp bends (≥ 5× cable diameter), pinch points, or obstructing rail travel.

Ensure latches are fully engaged at both ends; press the latch to release—do not pull on the cable.

NOTE

SAS signalling requires clean, direct connections between the HBA and the tape drive. Do not use adapters, or converters. For reliable operation, use certified, like-for-like SAS cables and keep runs as short as practical—**no more than 5 metres** (16.4 ft).

Connecting Fibre Channel Cables



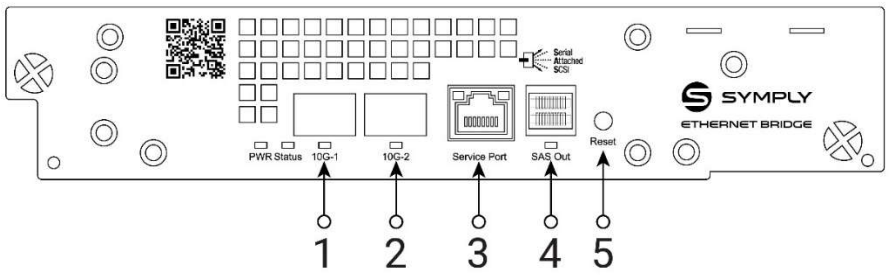
Number	Description
1	**Port A** – Connect this port only
2	Port B

1) Remove the FC port caps if necessary. Attach one end of the FC cable **to port A** on the tape drive.
2) Attach the other end of the FC cable to a switch or HBA.
3) It is recommended that you leave the FC port at the default settings of **Port Speed: Automatic** and **Port Type: Auto Detect**. With these settings, the tape drive will use the appropriate configuration.

Installing XTL Ethernet Module

The XTL Ethernet Module may be pre-installed at the factory.

Each XTL Ethernet Module occupies **one HH bay** and can bridge **up to four SAS LTO drives**.



Number	Description
1	Data Port 1
2	Data Port 2
3	Service Port
4	SAS Out (Connection to SAS Tape Drives)
5	Module Reset

1) **SAS link (Module → Drive)**
   Use the **supplied SAS cable** to connect the **SAS OUT** port on the **XTL Ethernet Module** to the external SAS port on the LTO drive (**port A**):

   a. **LTO-9 / LTO-10 library:** cable is **SFF-8644** ↔ **SFF-8644** (HD Mini-SAS ↔ HD Mini-SAS).

   b. **LTO-8 / LTO-7 library:** cable is **SFF-8644 ↔ SFF-8088** (HD Mini-SAS ↔ Mini-SAS).

2) **Port orientation**
   In **both cases**, the **SFF-8644** end goes to the **XTL Ethernet Module (SAS OUT)**. The opposite end mates with the LTO drive's SAS **port A** (SFF-8644 or SFF-8088, as fitted).
3) **Dress the cable**
   Coil and secure any excess length to the rack to avoid **strain** on the connectors. Maintain bend radius ≥ **10× cable diameter**; avoid kink/pinch points.
4) **Network uplinks (10GbE data ports)**
   Insert the **supplied SFP+ transceivers** into **Data Port 1** and **2** on the XTL Ethernet Module, then connect to your **host NIC(s)** or **10GbE switch**:
   a. **Optical:** SFP+ SR (LC) + LC-LC multimode fibre.
   b. **Copper:** SFP+ **10GBASE-T RJ45** module + Cat6a (or better) twisted pair. *(Use the option included with your kit; Data Ports are 10G-only ports.)*
5) **Management**
   Connect the **Management** Ethernet port to your management network for configuration/monitoring.
6) **Final checks**
   a. Verify all latches click/secure.
   b. Label both SAS and Ethernet runs.
   c. Keep SAS away from AC power leads where practical.

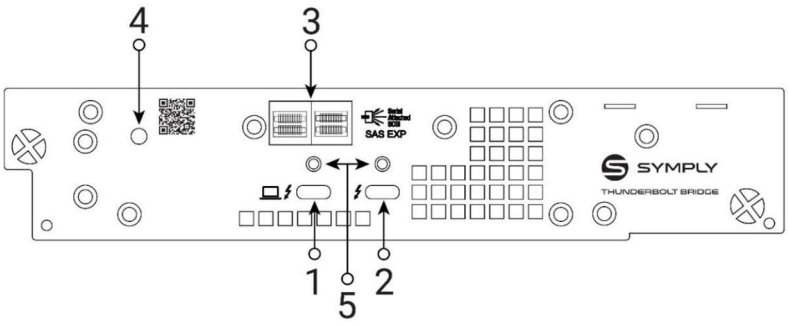
	**NOTE**	For information on configuring the XTL Ethernet Module please see the [SymplyPRO Ethernet Appliance User Guide].

	**MECHANICAL HAZARD**	**Danger:** Risk of hand pinching. Can trap hands, fingers and cause serious injury. Keep hands clear during operation.

Installing XTL Thunderbolt Module

The XTL Thunderbolt Module may be pre-installed at the factory.

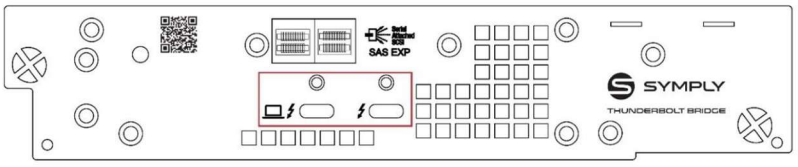
Each XTL Thunderbolt Module occupies **one HH bay** and can bridge **up to eight SAS LTO drives**



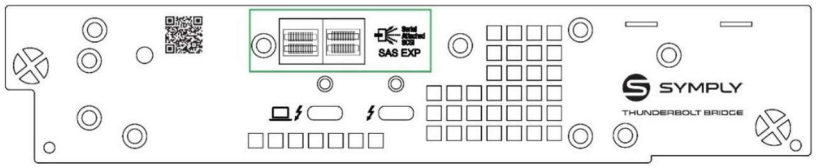
Number	Description
1	Thunderbolt 3 Port (15W)
2	Thunderbolt 3 Port (15W)
3	SFF-8644 SAS Ports (x2)
4	Ready Light (Green)
5	SymplyLOCK fixing point

Connector keying & strain relief: Thunderbolt and SAS connectors are **keyed**. Do **not** force a plug. Always secure the Thunderbolt cable with **SymplyLOCK** and dress cables to avoid strain on ports.

1) **Secure the Thunderbolt cable first**: Fit **SymplyLOCK** (supplied with the XTL Thunderbolt Module) to **either** Thunderbolt 3 port (as shown in the diagram). Insert the Thunderbolt cable fully, then tighten SymplyLOCK to retain the plug.



2) **SAS link: Module → Drive**: Use the **supplied SAS cable** to connect the XTL Thunderbolt Module to the LTO drive:
    a. **LTO-9 / LTO-10 library: SFF-8644 ↔ SFF-8644** (HD Mini-SAS ↔ HD Mini-SAS). **Port A.**
    b. **LTO-8 / LTO-7 library: SFF-8644 ↔ SFF-8088** (HD Mini-SAS ↔ Mini-SAS). **Port A.**
3) **Module-side connection**: In **all cases**, the **SFF-8644** end mates with the SFF-8644 port on the **XTL Thunderbolt Module**.



4) **Drive-side connection**: Connect the other end to the LTO drive's SAS port (**SFF-8644 or SFF-8088**, as fitted). Ensure the latch/screws engage. Always connect to **port A** on the LTO drive.
5) **Cable dressing**: Coil and **secure excess length** to the rack to minimize connector stress. Maintain a bend radius ≥ **10× cable diameter**; avoid pinch points and tight bends.
6) **Final checks**
    a. Verify Thunderbolt cable is **locked** with SymplyLOCK.
    b. Confirm SAS connectors are **fully seated** and retained.
    c. Label cables for future service.

	NOTE	For information on configuring the XTL Thunderbolt Module please see the [SymplyPRO Thunderbolt User Guide].

	**MECHANICAL HAZARD**	**Danger:** Risk of hand pinching. Can trap hands, fingers and cause serious injury. Keep hands clear during operation.

Powering On the XTL 8 and XTL 24

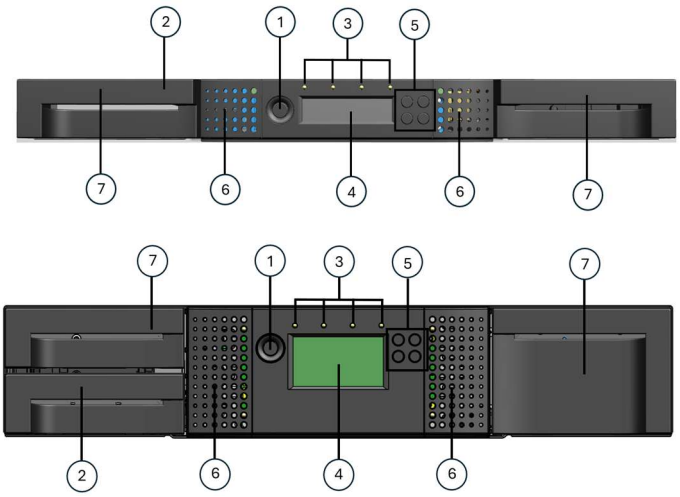
Before power on the SymplyPRO XTL

Before powering on the system, ensure that none of the ventilation holes, or fans are blocked, that there are no obstructions around the system blocking airflow, that the environment is within the specified operating conditions and that acclimatization time has been allowed for both the autoloader and the media.

Power on the SymplyPRO XTL

1) **Remove the shipping lock**.
2) Plug the power cables into the power connectors on each module and into power outlets.
3) To use the RMI, **connect an Ethernet cable** from the port on the Library controller to your network.
4) **Power on the library by pressing the power button on the front next to the OCP**; the green light will illuminate. When the library is powered on, preforms a POST, it inventories the tape cartridges in the magazines, checks the firmware version on all modules, configures the tape drives.

NOTE The Power On Self Test (POST) sequence and takes approximately 5 minutes.



Number	Description
1	Power Button
2	Left Hand Side Magazine (inc Mailslot)
3	Front Panel LED
4	Front Panel LCD
5	Control Buttons
6	Air Vents
7	Right Hand Side Magazine

Verifying the Host Connection

To verify the connections between the host computer and the library:

1. Install the application software and/or drivers that are compatible with the library. Backup software packages might require additional software or licensing to communicate with the robotics.
2. Verify the connection between the library and the host using the host server's operating system utilities.

Installing Windows Library and Tape Drivers

Prerequisites

- Hardware cabled and **powered on/ready** (let the library finish initializing).
- HBA/NIC/Thunderbolt drivers installed.
- **Point-to-point** for SAS/Thunderbolt
- **Switch or P2P** for FC/iSCSI.
- Multi-LUN/Report LUNs **enabled** so the host can see the drive (LUN 0) **and** robotics (LUN 1).

1) Confirm Windows sees the hardware

a. Open **Device Manager** → you should see entries under **Tape drives** and **Medium Changers**.

b. If only the tape drive appears (no Medium Changer): rescan, enable multi-LUN on the HBA/initiator, then reboot if needed.

2) Install the tape drive driver: Most backup apps require a vendor LTO driver (IBM). Some work with the in-box Microsoft driver.

1. Right-click the device under **Tape drives** → **Update driver**.
2. **Browse my computer** → point to the extracted vendor driver package → **Next**.
3. Reboot if prompted.

3) Install the library (robotics) driver: For Windows, use the **Microsoft "Unknown Medium Changer"** unless your software specifies a vendor driver.

1. In **Device Manager**, right-click the library (under **Medium Changers** or as **Unknown device**) → **Update driver**.
2. **Browse my computer** → **Let me pick from a list** → **Medium Changer devices** → select **Unknown Medium Changer** → **Next**.

4) iSCSI/FC notes (if applicable)

- **iSCSI:** Open **iSCSI Initiator** → **Discovery** (add portal to the XTL Ethernet Module) → **Targets** → **Connect** with **Enable multi-path off** for tape; tick **Add this connection to the list of Favourite Targets** (persistent).

- **Fibre Channel:** Zone the host HBA to the library/drive WWPNs; present **both** LUN 0 (drive) and LUN 1 (robotics).

5) Verify & hand off to software

- Recheck Device Manager: one (or more) **Tape drive(s)** + one **Medium Changer** present, all **Status: OK**.
- Start your backup/archive application and rescan devices. Restart its services if they were running during driver install.

The Windows drivers for the SymplyPRO XTL and Tape drives our available to download from [SymplyPRO XTL Drivers].



NOTE Symply suggest you check with your Application Software Vendor to determine the proper installation procedure for your configuration.

Many software partners provide their own drivers for use with libraries. Use of the drivers below may prevent your backup software from working properly.

Verifying the Installation

Verify that the library has the current firmware revision. The library firmware revision is displayed in the top left corner on the RMI screen or on the **Home > Status > Library > Library Status** screen on the OCP.

If necessary, update the library firmware from the OCP or RMI **Maintenance > Software Upgrades > System Firmware** screen.

After configuring the library, you can save the configuration settings to a USB flash drive from the OCP or to a file on your computer from the RMI **Configuration > Save/Restore** screen. Having a backup of the library configuration is helpful when recovering from a configuration error or if the library needs service.

Configuring Additional Features

The SymplyPRO XTL and XTL 24 have many features to provide a better user experience.

- Enabling the mailslot. See [Enabling or Disabling Mailslots].
- Naming the library via the partitioning wizard. See [Configuring Library Partitions].
- Partitioning the library. See [Configuring Library Partitions].
- Enabling and configuring SNMP network management. See [Configuring SNMP].
- Setting up email event notification. See [Configuring Event Notification Parameters].

Tape Cartridges and Magazines

This chapter explains which media to use with your library, and how to label and write-protect your tape cartridges. Careful labelling and handling of the tape cartridges will prolong the life of the tape cartridges and the library.

Using and Maintaining Tape Cartridges

Use the Ultrium data and cleaning tape cartridges designed for your model of library.

 **CAUTION**	Do not degauss LTO data cartridges! These data cartridges are pre-recorded with a magnetic servo signal. This signal is required to use the cartridge with the LTO tape drive. Keep magnetically charged objects away from the cartridge.

To maximise the life of your cartridges:

- **Use only approved media** for your device/model.
- **Clean the tape drive** when the **Clean Drive** LED illuminates (use an approved cleaning cartridge).
- **Handle with care**—do not drop cartridges; shock can damage the shell or internal tape media.
- **Avoid heat and sunlight.** Keep cartridges away from heaters, ducts, and direct sun.
- **Observe environmental limits.** Operating: **10–35 °C (50–95 °F).** Storage: –40 to +60 °C (–40 to +140 °F) in a dust-free, **20–80% RH environment.**
- **Acclimatise after extremes.** If a cartridge has been outside these limits, let it stabilise at room temperature for the **same duration** it was exposed (or **24 hours**, whichever is less) before use.
- **Keep away from electromagnetic sources.** Do not place cartridges near strong magnetic fields or EM sources (e.g., monitors, motors, speakers, X-ray equipment), which can destroy data and servo patterns.
- **Label correctly.** Apply identification labels **only** in the designated area.

Labeling Tape Cartridges

The library includes a barcode reader that scans cartridge labels and stores the resulting inventory in memory. This inventory is then presented to the **host application**, the **OCP**, and the **RMI**. Applying a barcode label to every cartridge is mandatory, as it lets the library identify media immediately and significantly reduces inventory time.

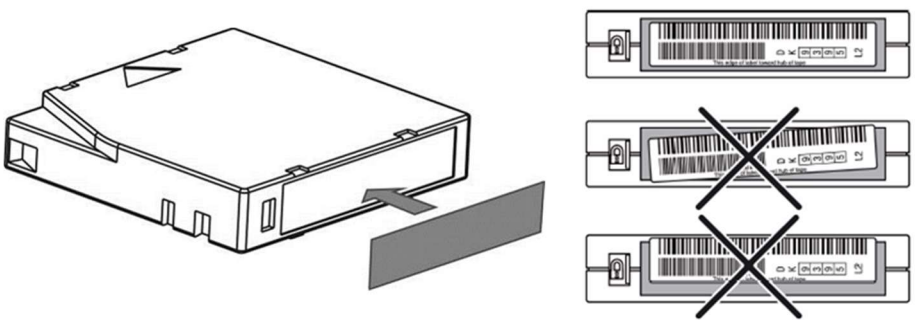
Use only high-quality labels. A correctly formatted LTO barcode ends with a **two-character media identifier** (e.g., **L9** for LTO-9, **L8** for LTO-8). The library enforces media compatibility using this suffix and will **not load incompatible media**—for example, a cartridge labelled as **LTO-7** will not be loaded into an **LTO-9** drive. This prevents time-consuming load attempts that would otherwise be rejected by the drive.

Your host software may track additional details against each barcode, such as:

- Date of format/initialisation.
- Media pool membership.
- Data set or job information stored on the tape.
- Backup age/retention status.
- Error history (to identify suspect or failing media).

!	**IMPORTANT**	Misusing and misunderstanding barcode technology can result in backup and restore failures. **Use only high-quality labels**. Self-printed labels are not recommended as they are often a source of barcode reading issues.

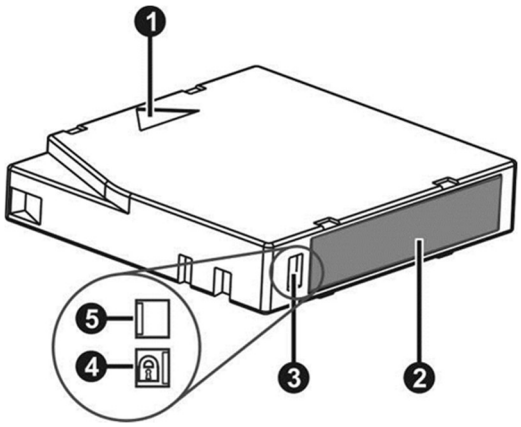
LTO tape cartridges have a recessed area located on the face of the cartridge next to the write-protect switch. Use this area for attaching the adhesive-backed bar code label. **Only apply labels as shown**:



!	**IMPORTANT**	• The barcode label should only be applied as shown, with the alphanumeric portion facing the hub side of the tape cartridge. • Never apply any label, anywhere else on the tape cartridge. This will cause the cartridge to jam in a tape drive. • Never apply multiple labels onto a cartridge because extra labels can cause the cartridge to jam in a tape drive.

Write Protecting Tape Cartridges

All rewriteable data cartridges have a **write-protect switch** to prevent accidental erasure or overwriting of data. Before loading a cartridge into the device, make sure the write-protect switch on the front of the cartridge is in the desired position.



Number	Description
1	Insertion Arrow
2	Barcode Label Area
3	Write-Protection Switch
4	Write-Protected
5	Write-Enabled

Read and Write Compatibility

Ultrium Read/Write Compatibility:

Number	LTO-7 Drive	LTO-8 Drive	LTO-9 Drive	LTO-10 Drive
LTO-5 Media	Read Only	Incompatible	Incompatible	Incompatible
LTO-6 Media	Read & Write	Incompatible	Incompatible	Incompatible
LTO-7 Media	Read & Write	Read & Write	Incompatible	Incompatible
LTO-8 Media	Incompatible	Read & Write	Read & Write	Incompatible
LTO-9 Media	Incompatible	Incompatible	Read & Write	Incompatible
LTO-10 Media	Incompatible	Incompatible	Incompatible	Read & Write

Barcode Reader

The barcode reader provides inventory feedback to the host application and/or LCD screen by reading the cartridge barcode labels. The library stores the customized inventory data in memory.

Magazines

Cartridges are stored in magazines.

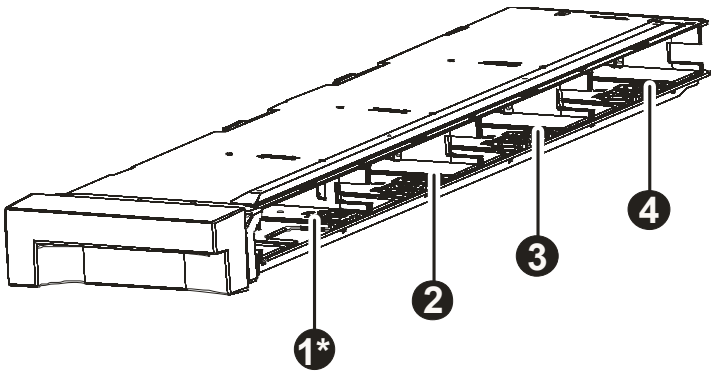
- Up to **4 cartridges** can be stored in each magazine for the **XTL-8**. Magazines may be removed and inserted individually.
- Up to **12 cartridges** can be stored in each magazine for the **XTL-24**. Magazines may be removed and inserted individually.

The SymplyPRO XTL 8 and XTL 24 have two removable magazines. Magazine access can be password protected. For safety reasons, the robotic motion is stopped when a magazine is removed. The magazines can be released using the Operator Control Panel (OCP) or the Remote Management Unit (RMU). In case the OCP or RMU initiated process has failed or the library no longer has power a manual emergency release is available.

!	**IMPORTANT**	To manually release a magazine, see [Using the Manual Release to Unlock Magazines]. However, this manual process should only be used if the magazine cannot be released using the Operator Control Panel or the Remote Management Unit.

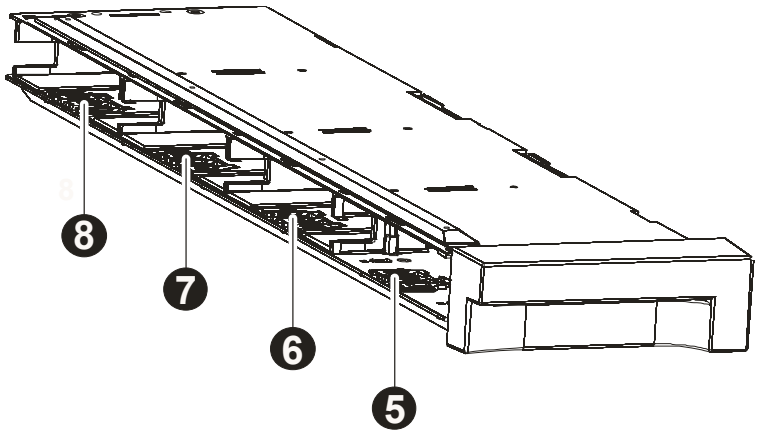
Inserting tape cartridges into a magazine

The slot numbering scheme is shown below for the **left magazine for the XTL 8.**

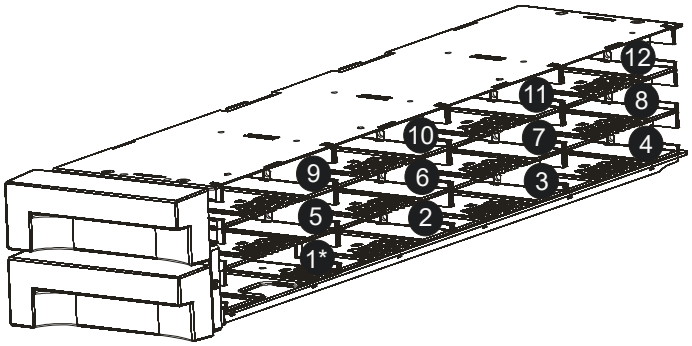


Slot #1 is the mailslot.

The slot numbering scheme is shown below for the **left magazine for the XTL 8.**

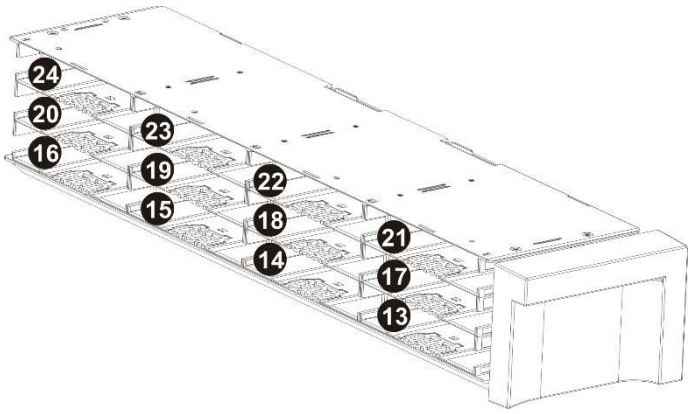


The slot numbering scheme is shown below for the **left magazine for the XTL 24**.



Slot #1 is the mailslot.

Slot numbering **right magazine for the XTL 24**.



Mailslots

Mailslots let you import/export individual cartridges without interrupting normal library operations. On the **XTL-8** and **XTL-24**, there is **one mailslot** located in the **left magazine** at **slot #1**. If the library is partitioned into multiple logical libraries (XTL 24 only), the mailslot can be **shared between partitions**.

If you request to open the mailslot while the robotics is busy, the command will be denied, and the display will show **Busy**. Wait until the current robotic operation finishes, then issue the command again.

The mailslot needs to be enabled using the RMU.

Initial Setup of the Library

Different Operating Modes of the SymplyPRO XTL 24

There are two basic modes that the OCP operates in.

- User Interaction Mode.
- System Drive Mode.

First is the User Interaction Mode. This mode is employed when a user is controlling the library via the buttons on the OCP on the front of the library.

The second mode is the System Driven Mode. This is the usual mode of operation, when the library is controller via backup or archive software running on the host server or workstation. In this mode, the OCP displays status associated with the actions that were caused from commands issued via the Drive's interface. Actions like Loading, Rewinding or Moving tape will be displayed.

When an OCP button is pressed and released, the OCP automatically transitions to User Interaction Mode. User Interaction mode will continue until 3 minutes after a user stops pushing buttons, or the requested robotic action stops - whichever is longer. At this time the OCP will return to System Driven Mode.

The SymplyPRO XTL 8 and XTL 24 includes a user security feature, which when activated restricts the User Interaction Mode access to the Information and Login menu item, until a login with correct PIN is entered.

Library Interfaces:

- **Operator Control Panel (OCP):** Monitor, configure, and control the library from the front panel.
- **Remote Management Interface (RMI):** With the RMI, you can monitor, configure, and control the library from a web browser. The RMI hosts a dedicated, protected Internet site that displays a graphical representation of the library.

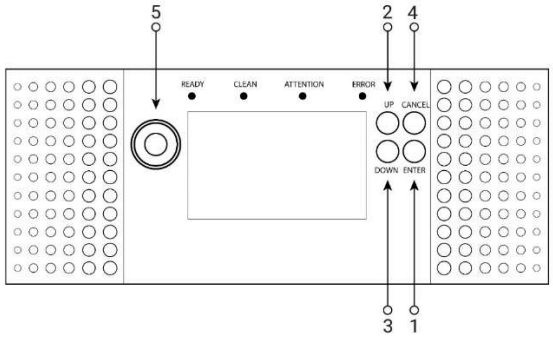
Using the OCP

The OCP on the front of the autoloader includes a 2-line by 16-character green back lit LCD, four function keys, and four LEDs. This panel provides everything that you need to monitor the autoloader status and control some functions.

The OCP has a power button, navigational buttons, an LCD screen, and four LEDs. With the OCP you can monitor, configure, and operate many autoloader functions from the autoloader front panel. To navigate the OCP, use the navigational, enter, and cancel buttons.

To power on the autoloader, press the power button. To power off the library, press the power button for five seconds and then release it.

With the four OCP buttons, you can traverse the OCP menu structure and enter information.



Number	Button	Description
1	Enter Button [↵]	The ENTER button to go to a sub menu or execute an action
2	Up Button [⇑]	The UP button is used to navigate through menu items
3	Down Button [⇓]	The DOWN button is used to navigate backward through menu item
4	Cancel Button [x]	The CANCEL button is used to cancel a user action and return to the last menu item
5	Power Button	Pressing the POWER ON/OFF button will initiate a controlled Power Down of the unit (soft power down)

OCP Default Credentials

These are the default PINs for OCP access

Description	Password
Standard User	0000
Administrator User	0000

Using the RMI

With the RMI, you can monitor, configure, and operate most library functions from a web browser.

When possible, it is recommended that the RMI be used as the primary library interface because the web interface provides access to additional features, includes online help, and is easier to use. However, the RMI is not required to use the product, except to configure advanced features, such as SNMP, IPv6, encryption, and partitions.

Before using the RMI, you must configure the library network settings with the OCP. This can be done with the Initial Configuration Wizard. See [`Using the Initial Configuration Wizard`].

To start the RMI, open the latest version of a supported HTML browser and enter the IP address of the library in the browser's address bar. Supported browsers include Internet Explorer, Firefox, Chrome and Safari.



TIP Check the online help in the RMI for additional information. The help pages are updated with firmware updates and often contain up-to-date technical details that might not be contained in this document. To access RMI help, click the **?** icon on the right side of the RMI top banner.

Remote Management Unit (Web Interface) Credentials

Username	Description	Password
Guest	Standard User	systd
Admin	Administrator User	syadm

Default IP Address

Management Port (GbE RJ45)	
IP Address	DHCP Default

The management port is set to DHCP, the resolved IP address can be accessed via the OCP display. View network Information:

- Use the Up/Down buttons to go to the Information/Status on the Home screen.
- Navigate with the Up/Down buttons to the Network.
- Note IP address.

Using the Initial Configuration Wizard on the OCP

Initial configuration steps on the OCP

1) **Log into the Operator Control Panel (OCP) as Administrator**
   (press any key > Select User: “ADMINISTRATOR” PIN:0000)
2) **2. Verify/Change network settings**
   (Configuration > Network)
3) **3. Set INITIAL RMI Password**
   (Configuration > Users > Reset RMI PW, Select User: “ADMINISTRATOR”)
   a. If one person physically installs the library and a second person will configure the library, share the network settings and INITIAL RMI Administrator password set in step 3 as appropriate.
4) **4. Log into the RMI**
   From a browser, log into the Remote Management Interface (RMI) as the Administrator user. (use the IP address from Step 2 and the Initial Password set in step 3)
5) **5. Change Password and setup partition**
   After logging in the first time, you will be prompted to set a new password, then you will be prompted that the library has no default partition. The library will remain OFFLINE to connected hosts until a valid partition is created.
6) **6. Create a partition using the Basic or Expert Partition Wizard**
   (Configuration > Partitions > Basic or Expert Wizard)
7) **7. Complete initial Configuration**
   (Complete any other configuration details required for your installation from the RMI, including date/time settings.)



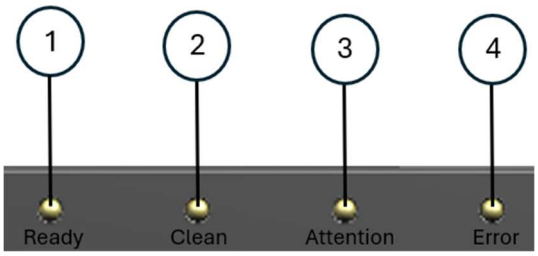
NOTE On the very first power up of the library the user is prompted to walk through the Initial Configuration wizard. It is recommended to walk completely through the wizard and finish the wizard by pressing the **Finish Button**. Otherwise with every login on the OCP the user will be prompted again to walk through the wizard.

Operating the Library using the Operator Panel

The OCP contains a power button, an LCD display, four navigation buttons, and four LEDs. With the OCP you can monitor, configure, and operate most library functions from the library front panel. To navigate the OCP, use the four navigation buttons (up/left, down/right, Enter, Back).

The OCP provides a subset of menu items compared to the full capability of the RMI. Menu items that are similar to the RMI are not described again in detail. For details, please refer to the corresponding item in the section [`Operating the library using the RMI`].

Front Panel LED Indicators



Number	LED	Colour	Description
1	Ready / Activity	Green	Illuminated when power is on. Blinking when there is tape or autoloader robotics activity.
2	Clean Drive	Amber	Illuminated when the tape drive has determined that a cleaning cartridge should be used. Cleaning is only necessary when the autoloader directs you to do so. Additional cleaning is not necessary. The LED will be turned off after the tape drive is cleaned successfully.
3	Attention	Amber	Illuminated if the autoloader has detected a condition that requires attention by the operator. Media might be bad, marginal or invalid. It will be cleared when all invalid cartridges have been exported from the tape autoloader.
4	Error	Amber	Illuminated if an unrecoverable tape drive or autoloader error occurs. A corresponding error message displays on the LCD screen (see for more information). It will be cleared when the error state is resolved.

OCP start screen



OCP Login

1) If the OCP start screen is on, press **Enter** to get to the login screen
2) On the Login screen press **Up/Down** and select the **User** pressing **Enter**
3) Then press **Enter** and enter the 4-digit PIN with pressing **Up/Down** to change numbers.
4) Afterwards the Information/ Status screen appears



Magazine States

After a magazine has been opened and closed, a library inventory will be performed.

NOTE

1. If a magazine unlock is in process, no other magazines or mailslots can be unlocked.
2. If an unlocked magazine is not opened within 30 seconds, the magazine will be locked.

Operations via OCP

Navigate with the **Up/Down** buttons to the **Operation** menu entry on the **Home screen** to access the operation features.

The Operation Menu provides the following submenus:

- **Magazine Unlock Left**
- **Magazine Unlock Right**
- **Mailslot Unlock**

Magazine Unlock Left

1) After pressing **Enter** at the Operation Menu the Magazine Unlock Left screen appears.
2) Press **Enter** and the Magazine can be pulled out.

! IMPORTANT Wait before pulling out the magazine until the LED is quickly flashing and OCP message says that the magazine is unlocked

NOTE

- Opening a magazine will take the library off-line.
- The magazines will relock after 30 seconds.

Magazine Unlock Right

1) After pressing **Enter** at the Operation Menu the Magazine Unlock Left screen appears.
2) Press the **Up/Down** buttons and the Magazine Unlock Right screen appears.
3) Press **Enter** and the Magazine can be pulled out

!	**IMPORTANT**	Wait before pulling out the magazine until the LED is quickly flashing and OCP message says that the magazine is unlocked

	NOTE	• Opening a magazine will take the library off-line. • The magazines will relock after 30 seconds.

Mailslot Unlock

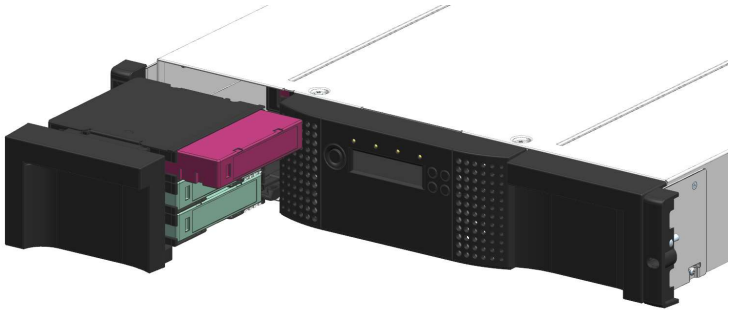
The Mailslot Unlock screen must be enabled on the RMI before it is available in the OCP. See [Enabling or Disabling Mailslots]

1) After Enabling the Mailslot in the RMI and pressing **Enter** at the Operation Menu.
2) Press the **Up/Down** buttons and the **Mailslot Unlock** screen appears.
3) Press **Enter** and the Mailslot will open.
4) Push the Mailslot back in the library and the mailslot is locked again.

Mailslot on XTL 8



Mailslot on XTL 24



Configuration via OCP

Navigate with the **Up/Down** buttons to the **Configuration** menu entry on the **Home screen** to access the configuration features.

The **Configuration** Menu provides the following submenus:

- **Library**
- **Network**
- **Users**

Library Configuration

After pressing **Enter** at the Configuration Menu the **Library** screen appears.

The Library Menu provides the following submenus:

- **Reset to Default Settings**
- **Reset to manufacturing**

Reset to Default Settings

1) After pressing **Enter** at the **Library** Menu the **Reset to Default Settings** screen appears.
2) Press **Enter** to reset to default settings.

Reset to Manufacturing Default

1) After pressing **Enter** at the **Library** Menu the **Reset to Default Settings** screen appears.
2) Press **Up/Down** buttons and the **Reset to Manufacturing** screen appears.
3) Press **Enter** to reset to manufacturing.

Network

1) After pressing **Enter** at the Configuration Menu the **Library** screen appears.
2) Press **Up/Down** buttons and the **Network** screen appears.

The Library Menu provides the following submenus:

- **IPv4 Mode DHCP**
- **IPv4 Mode STATIC**

IPv4 Mode DHCP

1) After pressing **Enter** at the **Network** Menu the **IPv4 Mode DHCP** screen appears.
2) Press **Enter** and the Disable ? **Yes/No screen** appears.
3) Press **Up/Down** and select **Yes** or **No** and press **Enter.**

IPv4 Mode STATIC

1) After pressing **Enter** at the **Network** Menu the **IPv4 Mode DHCP** screen appears.
2) Press **Up/Down** buttons and the **IPv4 Mode STATIC** screen appears.
3) Press **Enter** and the Disable ? **Yes/No screen** appears.
4) Press **Up/Down** and select **Yes** or **No** and press **Enter.**

Users

1) After pressing **Enter** at the Configuration Menu the **Library** screen appears.
2) Press **Up/Down** buttons and the **Users** screen appears.

The Library Menu provides the following submenus:

- **Reset RMI PW**
- **RMI Restricted Login**
- **Configure PIN**

Reset RMI PW

1) After pressing **Enter** at the **Users** Menu the **Reset RMI PW** screen appears.
2) Press **Enter** to reset the RMI PW.

RMI Restricted Login

1) After pressing **Enter** at the **Users** Menu the **Reset RMI PW** screen appears.
2) Press **Up/Down** buttons and the **RMI Restricted Login** screen appears.
3) Press **Enter** for RMI Restricted Login.

Configure PIN

1) After pressing **Enter** at the **Users** Menu the **Reset RMI PW** screen appears.
2) Press **Up/Down** buttons and the **Config PIN** screen appears.
3) Press Enter and the **New PIN** screen appears.
4) Press **Up/Down** buttons to change numbers and press **Enter** to move forward until Verify PIN screen appears.
5) Repeat the new PIN and press **Enter.**

Maintenance via OCP

Navigate with the **Up/Down** buttons to the **Configuration** menu entry on the Home screen to access the configuration features.

The **Maintenance** Menu provides the following submenus:

- **Restore Config from USB**
- **Save Log to USB Device**
- **Update Firmware from USB Device**
- **Save Drive Dump to USB Device**
- **Upgrade Drive from USB Device**

Restore Config from USB

1) After pressing **Enter** at the **Maintenance** Menu the **Restore Config from USB** screen appears.
2) Press **Enter** and the Insert USB Device screen appears.
3) Insert the USB Device and press **Enter.**

Save Log to USB Device

1) After pressing **Enter** at the **Maintenance** Menu the **Restore Config from USB** screen appears.
2) Press **Up/Down** buttons and the **Save Log to USB Device screen** appears.
3) Press **Enter** and the **Insert USB Device screen** appears.
4) Insert the **USB Device** (in the rear controller module USB port) and press **Enter.**

Update Firmware from USB Device

1) After pressing **Enter** at the **Maintenance** Menu the **Restore Config from USB** screen appears.
2) Press **Up/Down** buttons and the **Update Firmware from USB Device** screen appears.
3) Press **Enter** and the **Insert USB Device screen** appears.
4) **Insert** the **USB Device** (in the rear controller module USB port) and press **Enter.**

Save Drive Dump to USB Device

1) After pressing **Enter** at the **Maintenance** Menu the **Restore Config from USB** screen appears.
2) Press **Up/Down** buttons and the **Save Drive Dump to USB Device** screen appears
3) 3. Press **Enter** and the **Insert USB Device** screen appears.
4) **Insert the USB Device** (in the rear controller module USB port) and press **Enter**

Upgrade Drive from USB Device

1) After pressing **Enter** at the **Maintenance** Menu the **Restore Config from USB** screen appears.
2) Press **Up/Down** buttons and the **Upgrade Drive from USB Device** screen appears.
3) Press **Enter** and the **Insert USB Device screen** appears
4) **Insert the USB Device** (in the rear controller module USB port) and press **Enter**

Information/Status in OCP

Use the **Up/Down** buttons to go to the **Information/Status** on the Home screen to access the status information.

The **Information/Status** Menu provides the following submenus:

- **Library Status**
- **Network Status**
- **Drive 1 Status**
- **Drive 2 Status** (XTL 24 Only)

Library Status

1) After pressing **Enter** at the **Information/Status** Menu the **Library Status** screen appears.
2) Press **Enter** and press **Up/Down** to navigate.

The **Library Status** Menu provides the following information:

- **Inventory**
- **Moves**
- **Power On Time**
- **Max Temperature**
- **Slots Empty**
- **Vendor ID**
- **Product ID**
- **Library Name**
- **Firmware Version**
- **Serial Number**
- **MAC Address**
- **Magazine Inventory**

Network Status

1) After pressing **Enter** at the **Information/Status** Menu the **Library Status** screen appears.
2) Press Up/Down buttons and the **Network Status** screen appears.
3) Press **Enter** and press **Up/Down** to navigate.

The **Network Status** Menu provides the following information:

- **Protocol IPv4**
- **DHCP Enabled** (Yes/No)
- **IPv4 Address**
- **IPv4 Netmask**
- **IPv4 Gateway**
- **WWNN**

Drive 1 Status

1) After pressing **Enter** at the **Information/Status** Menu the **Library Status** screen appears.
2) Press Up/Down buttons and the **Drive 1 Status** screen appears.
3) Press **Enter** and press **Up/Down** to navigate.

The **Drive 1 Status** Menu provides the following information:

- **LTO Generation**
- **Vendor ID**
- **Activity**
- **Load Status** (No Medium / Medium)
- **Enabled** (Yes / No)
- **LUN Master** (Yes / No)
- **Port A Connected**
- **Port A Speed**
- **Port A Type**
- **Port A ID**
- **Port B Connected**
- **Port B Speed**
- **Port B Type**
- **Port B ID**
- **Product ID**
- **LTO Generation**
- **Interface Type**
- **Drive(s) Inventory**
- **Temperature (C)**
- **Powered**
- **Load Status**
- **Product ID**

Drive 2 Status

1) After pressing **Enter** at the **Information/Status** Menu the **Library Status** screen appears.
2) Press Up/Down buttons and the **Drive 2 Status** screen appears.
3) Press **Enter** and press **Up/Down** to navigate.

The **Drive 2 Status** Menu provides the following information:

- **LTO Generation**
- **Vendor ID**
- **Activity**
- **Load Status** (No Medium / Medium)
- **Enabled** (Yes / No)
- **LUN Master** (Yes / No)
- **Port A Connected**
- **Port A Speed**
- **Port A Type**
- **Port A ID**
- **Port B Connected**
- **Port B Speed**

- **Port B Type**
- **Port B ID**
- **Product ID**
- **LTO Generation**
- **Interface Type**
- **Drive(s) Inventory**
- **Temperature (C)**
- **Powered**
- **Load Status**
- **Product ID**

Logout OCP

1) Use the **Up/Down** buttons to go the **Logout** on the Home screen to access the **Logout** screen.
2) Press **Enter** and the **Logout Yes/No** screen appears.
3) Press **Up/Down** and **select Yes or No** and press **Enter.**

Operating the library using the RMI

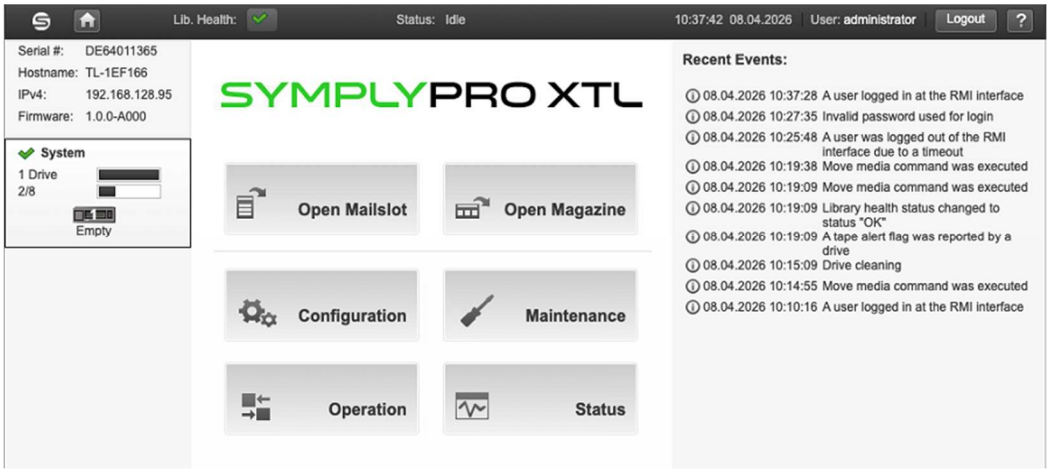


The library needs cartridges before performing data read and write operations, or any tests or operations that transfer cartridges.

Using the Library Main Screen on the RMI

The Library main screen is organized into the following regions:

- **Top Banner** - Contains the home button and displays the overall status and information about the library and user.
- **Left Pane** - Displays the library identity and system status.
- **Centre Pane** - Provides access to operate and configure the library and to view additional status information.
- **Right Pane** - Displays a log of recent events.



Top Banner Elements

Icon	Type	Description
	Home	Returns to the library main screen
	Library Health	The green check mark Status OK icon indicates that all library components are fully operational and that no user intervention is required.
	Library Health	The yellow triangle exclamation point Status Warning icon indicates that user attention is necessary, but that the library can still perform most operations. Click the icon to display the event ticket log.
	Library Health	The red circle X Status Error icon indicates that user intervention is required, and the library is not capable of performing some operations. Click the icon to display the event ticket log.
Status of Library	Idle	The library robotic is ready to perform an action
Status of Library	Moving	The library robotic is moving a cartridge.
Status of Library	Scanning	The library robotic is performing an inventory of cartridges.
Status of Library	Offline	The library robotic has been taken offline by the library.
Library Time & Date		Helpful when analysing event logs and support tickets and might be needed when contacting support.
User		The user account for this session.
Logout		Logs out of this session.
?		Accesses online help.

Left Pane Elements

Library Status – Overall library confirmation and status	
Serial #	The Base Module serial number
Hostname	The library hostname
Network Configuration	The IP version (IPv4 or IPv6) and IP address
Firmware	The library firmware version

Library Status Overview

Library Status Overview: A summary of system health. Click the system status area to select the system.		
	Library Health	The green check mark Status OK icon indicates that the library and each of its components are fully operational and that no user intervention is required.
	Library Health	The yellow triangle explanation point Status Warning icon indicates that user attention is necessary, but that the library can still perform most operations.
	Library Health	The red circle X Status Error icon indicates that user intervention is required, and the library cannot perform some operations.
Drive Status	The number of drives installed in the library and the health of each drive. Click on the drive to display drive configuration and status information in the centre pane.	
		A black square indicates that the drive is fully operational and that no user intervention is required.
		A yellow square indicates that user attention is necessary, but that the drive can still perform most operations.
		A red square indicates that user intervention is required, or the drive cannot perform some operations.
Magazine Slot Usage	The number of cartridge slots available and the number in use.	
Drive Operation Status	The current drive activity for each drive in the module. The drive operation status is only displayed for the selected module.	
	Write	The drive is performing a write operation
	Read	The drive is performing a read operation.
	Idle	A cartridge is in the drive, but the drive is not performing an operation.
	Empty	The drive is empty.
	Encryp	The drive is writing encrypted data.

Centre Pane Elements

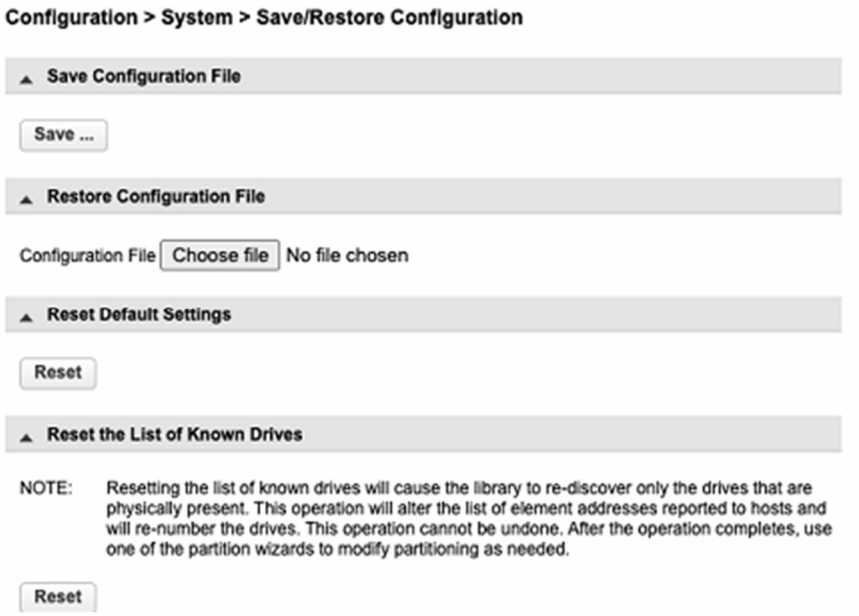
Item	Description
Open Mailslot	(Administrator user only) Click to unlock the mailslot on the selected module. Mailslots must be enabled before the slots can be used as mailslots. See [Enabling or Disabling Mailslots].
Open Magazine	(Administrator user only) Click to unlock a magazine in the selected module. Only one magazine in the library can be open at a time. See [Opening a Magazine].
Configuration	(Administrator user only) Click to configure the library. See [Configuring the Library].
Maintenance	(Administrator user only) Click to access maintenance functions. See [Maintaining the Library].
Operation	(Administrator user only) Click to access operation functions. See [Operating the Library].
Status	Click to access status information. See [Viewing Status Information].

Configuring the Library on the RMI

Saving, Restoring and Resetting the Library Configuration

From the **Configuration > System > Save/Restore Configuration** screen you can save the library configuration settings to a file, restore the settings, or reset the library configuration to the default settings. The saved configuration database will make it easier to recover the library configuration if you need to replace the Library Controller.

The feature **Reset the List of Known Drives** will do a re-discovery of installed hardware components.



Saving the library configuration to a file

1) Navigate to the **Configuration > System > Save/Restore Configuration** screen as shown above.
2) Click **Save.** Starts to download the configuration file to the browser or system running the RMI

Restoring the library configuration from a file

1) Navigate to the **Configuration > System > Save/Restore Configuration** screen.
2) Click **Browse** to navigate to and select the configuration file. The file must be a zip file.
3) Select the file and press **Upload File & Restore.** Starts the uploading process and restores the configuration file from the system running the RMI.

Resetting the default settings

To reset the library configuration to the default settings, click **Reset Default Settings**. For the default settings, see [Defaults and Restore Defaults Settings].

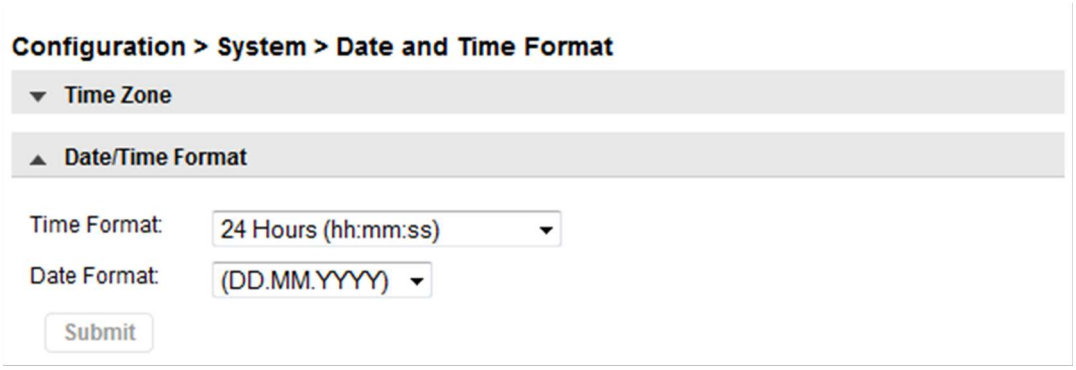
Resetting the List of Known Drives and Modules

To reset the List of Known Drives and Modules, click **Reset**. Removes not present Drives from the library.

Configuring the Date and Time Format

To configure date and time format parameters and to use an SNTP server, from the Configuration area, navigate to the **System > Date and Time Format** screen.

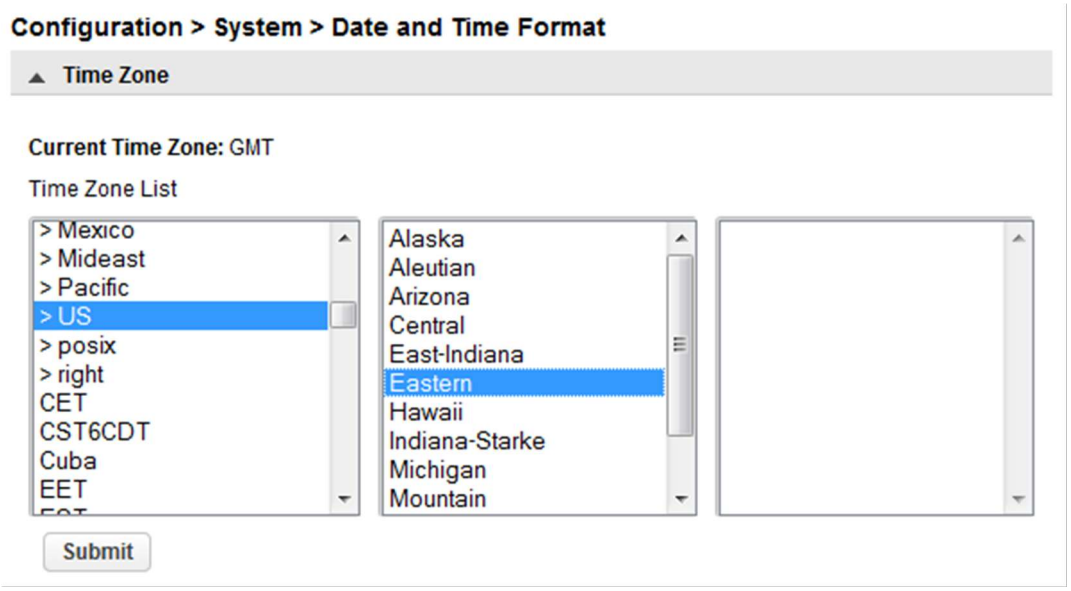
	NOTE	The library does not adjust its time for daylight saving time; the time must be adjusted manually.



Setting the Time Zone

1) Click **Time Zone**.

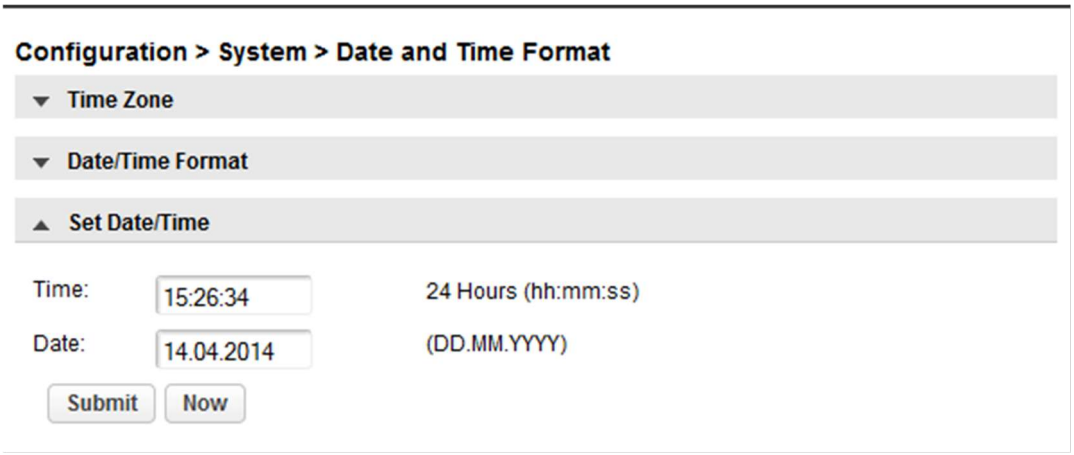
   A list of continents, countries, and regions is displayed. When an item proceeded with '>', for example> **US**, is selected, a submenu is displayed in the next column.



2) Expand the time zone list, as necessary, until a location with the appropriate time zone is visible.
3) Select a location with the appropriate time zone.
4) Click **Submit**.

Setting the Date and Time Format

1) Click **Date/Time Format**.



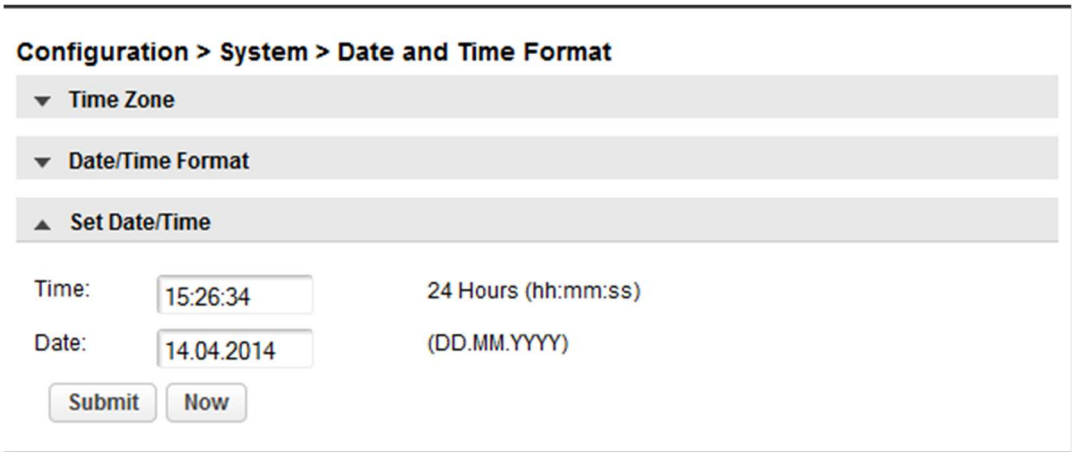
4) Select a time format.
5) Select a date format:
6) For example, July 30, 2025 is displayed as:

    a. DD.MM.YYYY - 30.07.2025
    b. MM/DD/YYYY - 07/30/2025
    c. YYYY-MM-DD - 2025-07-30

7) Click **Submit**.

Setting Date and Time

1) Click **Set Date/Time**.

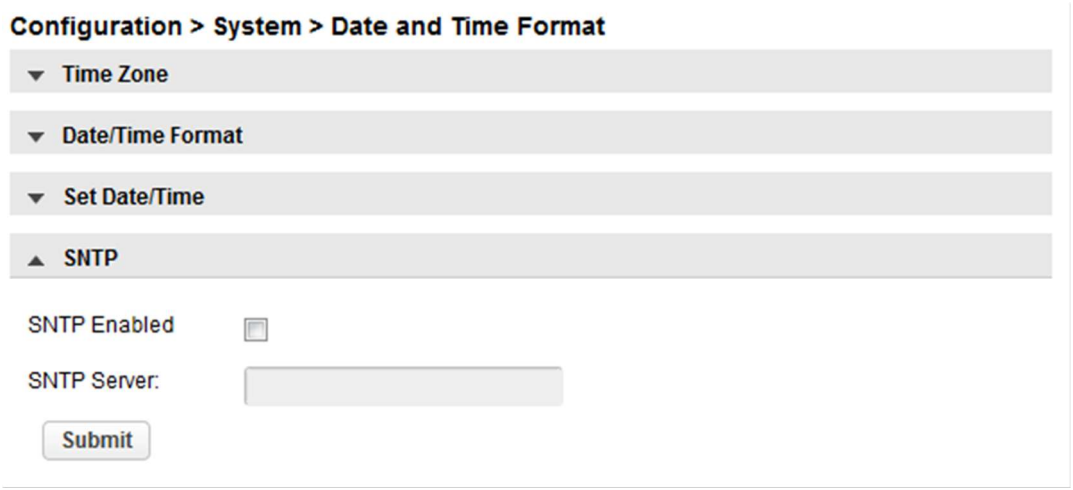


2) Enter time and date in given format or use "Now" button to take over current time from local PC.
3) Click **Submit**.

Enabling SNTP (Simple Network Time Protocol) Synchronization

The library must have network access to an SNTP server.

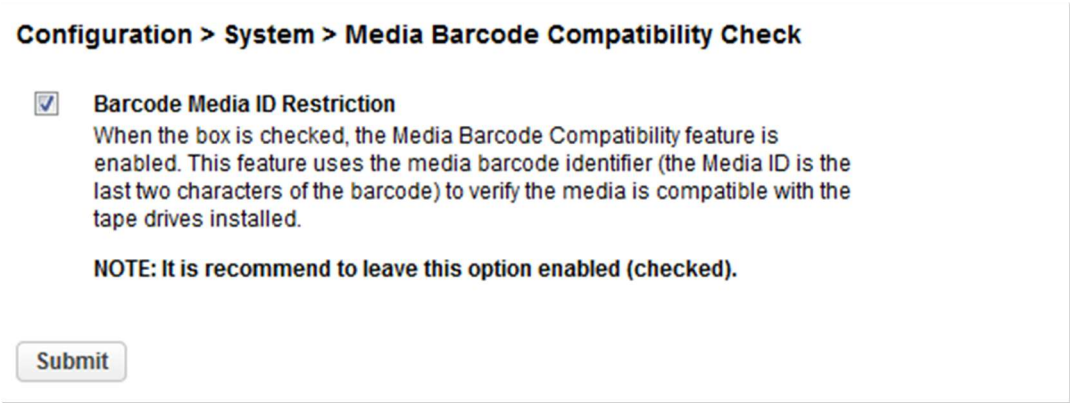
1) Click **SNTP**.



2) Click **SNTP Enabled**.
3) Enter the SNTP server address.
4) Click **Submit**.

Configuring Media Barcode Compatibility Checking

From the **Configuration > System > Media Barcode Compatibility Check** screen you can enable or disable the barcode media ID check.



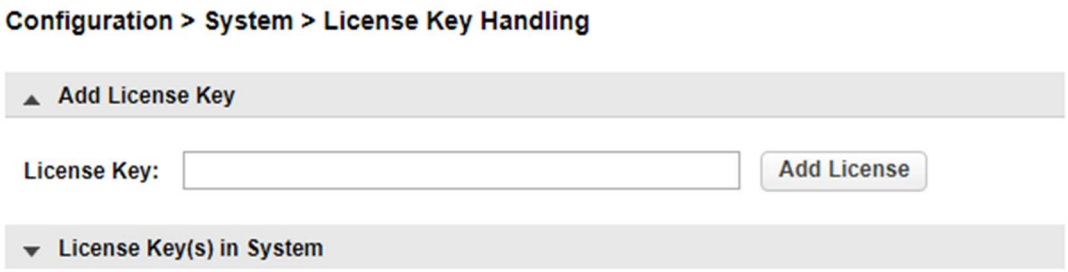
When **Barcode Media ID Restriction** is enabled, the library will only allow appropriate tape cartridges to be loaded into tape drives. The barcode media ID is the last two characters of the barcode. For example, an LTO-9 labelled cartridge will not be allowed to move into an LTO-7 tape drive.

When disabled, the library will move any tape to any tape drive. If the cartridge is incompatible with the tape drive, the library will display a message.

NOTE It is strongly recommended that all cartridges have barcode labels with the correct media ID, and that the Barcode Media ID Restriction is enabled.

License Key Handling

To add a license key, navigate to the **System > License Key Handling** screen.



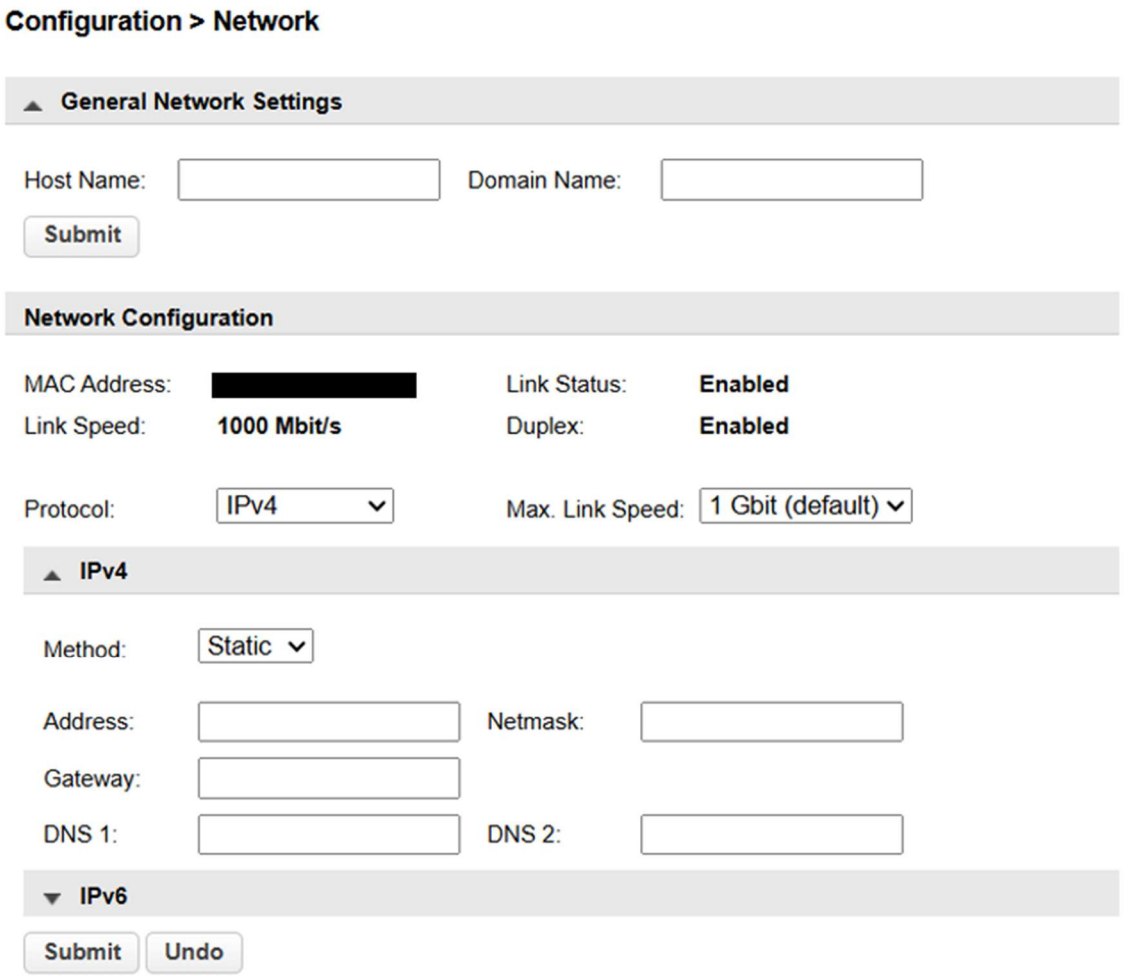
Add a license key

1) Enter license key. The license key needs to have a length of 15 characters
2) Click **Add License**

NOTE Once the license key is entered, the according information will appear in the list showing license keys in the system

Configuring the Library Network Settings

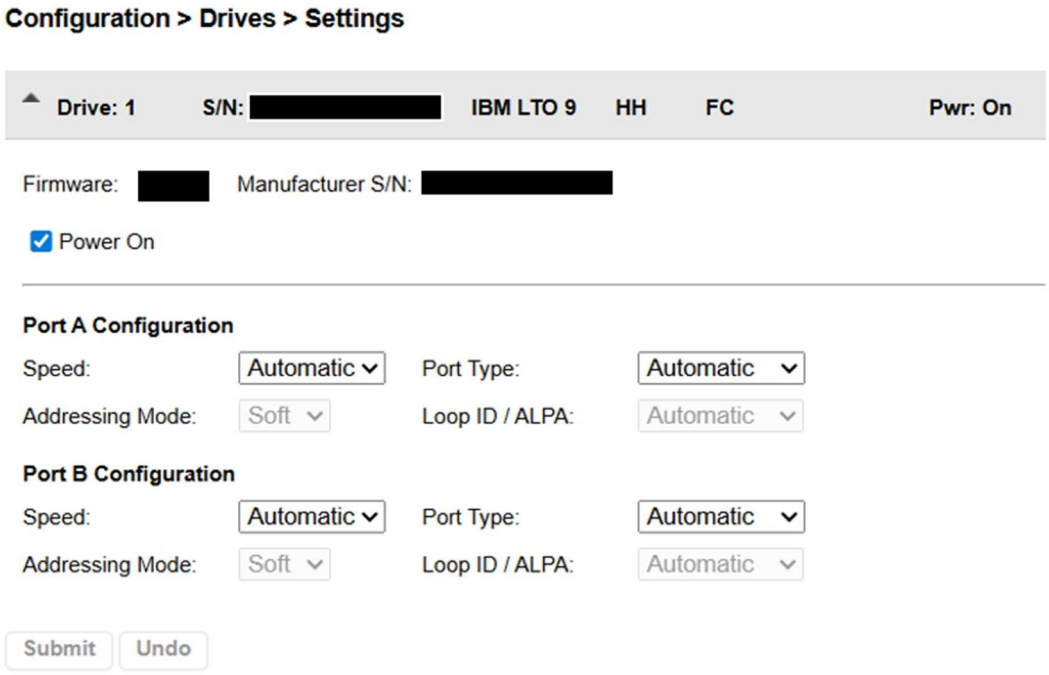
From the **Configuration > Network** screen you can configure the library network settings.



1) Navigate to the **Configuration > Network** screen.
2) Configure or update the **Host Name** and **Domain Name**. The RMI URL is *<Host Name>.<Domain Name>*.
3) Select the internet protocol to use for the library.
4) Configure the settings for the selected internet protocol.
5) To have the library obtain an internet address from a DHCP server, select the DHCP or Stateless method.
6) Click **Submit**.

Configuring Tape Drives

From the **Configuration > Drives** screen you can see and modify drive configuration.



- **Drive number** – Drives are numbered from the bottom of the library up beginning with one. The drive currently hosting the SCSI communication for the library is designated with (LUN).
- **Serial Number** – The serial number assigned to the tape drive by the library. This serial number is reported to host applications. The serial number cannot be modified.
- This is not the serial number assigned to the drive by the manufacturer; the serial number assigned by the manufacturer is shown in Manufacturer S/N.
- **LTO generation**
  - LTO 7 Ultrium Tape Drive
  - LTO 8 Ultrium Tape Drive
  - LTO 9 Ultrium Tape Drive
  - LTO 10 Ultrium Tape Drive
- **Drive form factor**
  - HH – half height
- **Drive interface**
  - FC – Fibre Channel
  - SAS – Serial Attached SCSI
- **(Modified)** – When present indicates that a setting has been changed. To apply the changes, click **Submit**. To reset all changed fields to their previously saved values, click **Undo**.

- **Pwr** – Indicates whether the drive is currently powered on or off.
- **Firmware** – The version of firmware currently installed on the drive.
- **Manufacturer S/N** – The serial number assigned to the drive when it was manufactured. Use this serial number when working with your Service.
- **Power On** – Checked when the drive is powered on.



NOTE Always power off a tape drive before removing it from the library or moving it to a new location within the library.

- **Port configuration** (FC only) – Drive port configuration.
  - **Speed** –The currently selected ◦ speed. The default is Automatic.
  - **Port Type**
    - **Automatic**
    - **Loop** – Enables selection of the Addressing Mode.
    - **Fabric**
  - **Addressing Mode** – When Port Type is set to Loop, Addressing Mode can be set to **Soft**, **Hard**.
  - **ALPA** – When Addressing Mode is set to Hard, you can choose an ALPA address from the drop-down list.

To modify the configuration of one or more tape drives:

1) Modify any of the configurable values.
2) Click **Submit**.



NOTE To configure the number of barcode characters to report to the host application and whether to report them from the left or right end of the label, use either the Basic Partition Wizard or Expert Partition Wizard. See [Using the Basic Partition Wizard] or [Using the Expert Partition Wizard].

Enabling or Disabling Mailslots

The **Configuration > Mailslot** screen lists each of the mailslots and shows whether each is enabled or disabled. To change the state, click the button for the mailslot and then click **Submit**. Slots not enabled as mailslots are available as storage slots.



Configuring Web Management

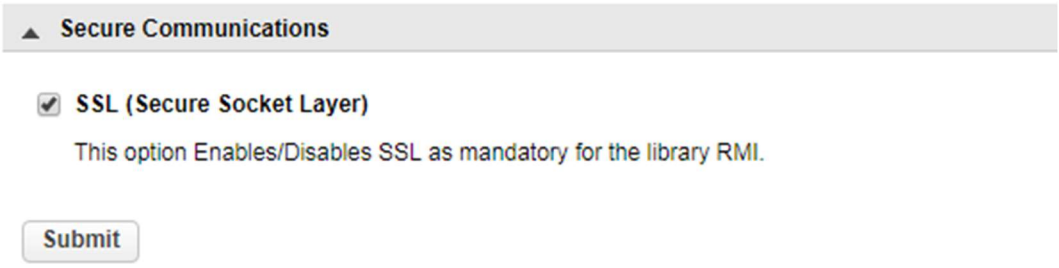
From the **Configuration > Web Management** screen you can set or modify the following web management features:

- SSL Secure Communication
- Certificate Setting
- Create Custom Certificate/Certificate Wizard
- Backup/Restore Custom Certificate
- Session Timeout and Session Locking
- Restricted RMI Login

Configuring SSL Secure Communication

From the **Configuration > Web Management** screen you can enable or disable secure access to the RMI using Secure Socket Layer (SSL). When SSL is enabled, connections to the RMI must use HTTPS.

Per default SSL is disabled.

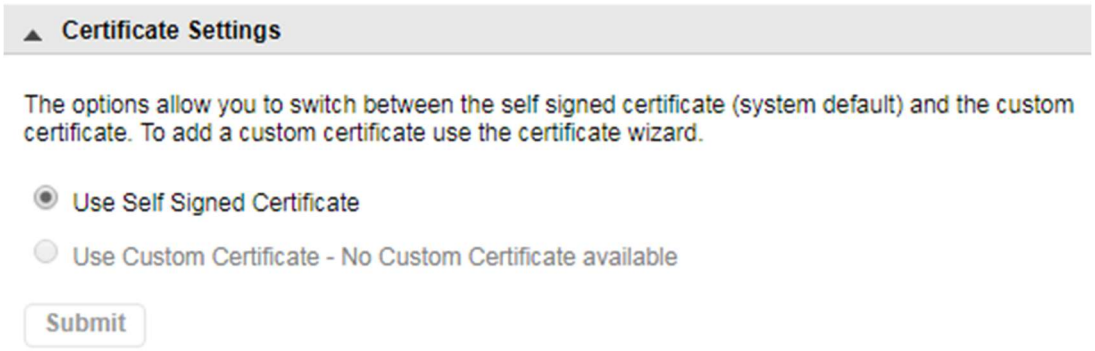


Configuring Certificate Setting

This screen provides the option to switch between the self-signed certificate and the custom certificate.

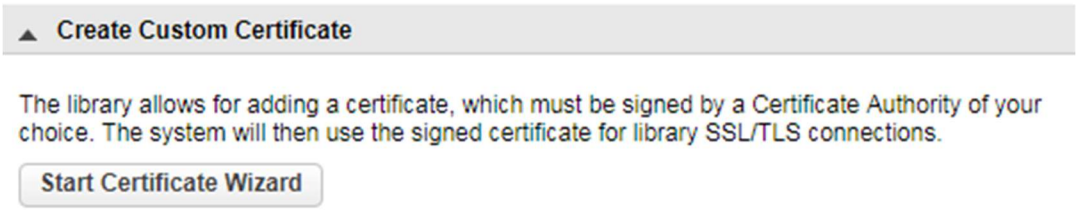
Per default the self-signed certificate is set.

To add a custom certificate, use the certificate wizard.



Create Custom Certificate by using the Certificate Wizard

The **Create Custom Certificate** screen allows to add a certificate, which must be signed by a Certificate Authority of your choice. The system then will use the signed certificate for SSL/TLS connections. The certificate will be used by the library for HTTPS connections to the RMI.



Before starting the wizard, prepare your Certificate Authority to sign the certificate. You will be pasting the certificate generated by the wizard into a field in the Certificate Authority for signing.

To start the Certificate Wizard, click the **Start Certificate Wizard** button. The wizard will guide you through adding a certificate to the library.

1) Read the **Information** screen and then click **Next**.
2) In the **Certificate Signing Request** screen create the certificate.
    a. Enter the information about the library and organization.
    b. Click **Generate CSR**.
3) Use a web browser copy command, such as **Crtl-c** to copy the certificate generated by the wizard is now in your computer's copy buffer.
4) Paste the certificate into the appropriate field in your Certificate Authority and then have the Certificate Authority sign the certificate.
5) In the wizard **Certificate Signing Request** screen, click **Next**.
6) In the **Signed Certificate** screen, paste the signed certificate into the **Signed Certificate** pane and then click **Finish**.
7) To verify that the certificate is being used, open an https connection to the library from a server or computer where the server-side certificate has been imported.

	NOTE	To clear the wizard settings when no longer using this certificate or reset the wizard configuration to its default state, click **Clear All Wizard Settings** on the **Information** screen

Configuring Backup/Restore Custom Certificate

Use the **Backup Custom Certificate** Button to download a backup of the currently installed certificate.

Use the following sequence to restore a previously saved certificate file:

- Select the certificate file you want to restore
- Click the **Restore Custom Certificate** button

Configuring Session Timeout and Session Locking

The **Session Timeout** screen allows to select how many minutes a user should stay logged in (5 or 30 minutes).

	NOTE	The timeout is only selectable for RMI. The timeout for OCP is always set to 5 Minutes

The **OCP/RMI Session Locking** screen allows to enable OCP/RMI session locking by clicking the checkbox. The library only supports one OCP or RMI session at a time for the Administrator, Service and Security users. With OCP/RMI session locking enabled, the library will not allow a new Administrator, Service and Security user login until a current session is logged out or times out.

	NOTE	When this setting is enabled, always logout of the RMI or OCP when finished with a session. Otherwise, no new sessions will be allowed until the current session times out.

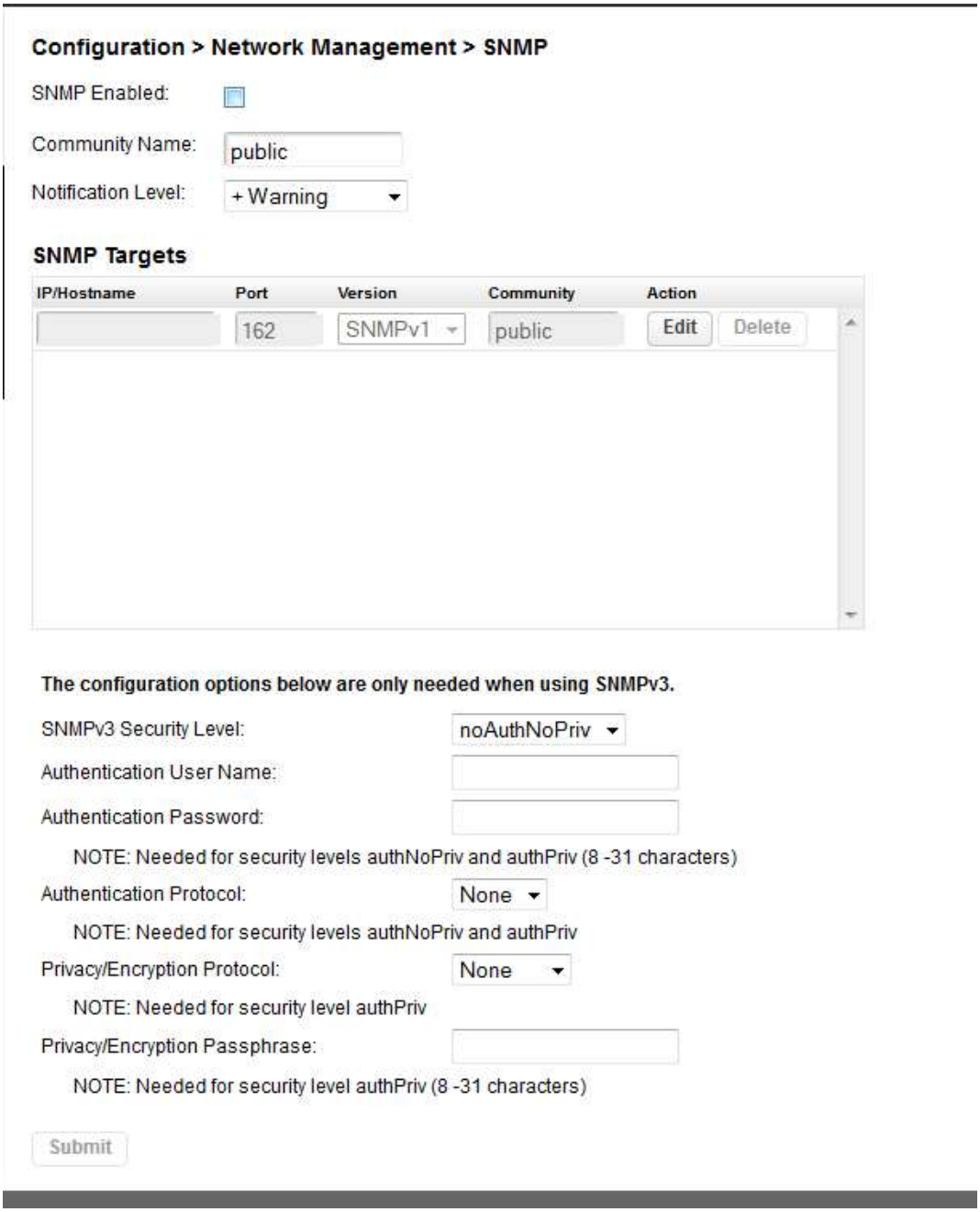
Configuring Network Management

From the **Configuration > Network Management** screen you can set or modify the following network management features:

- SNMP
- Event Notification (SMTP)
- Remote Logging (rsyslog)

Configuring SNMP

Use the **Configuration > Network Management > SNMP** screen to enable and configure SNMP (Simple Network Management Protocol), which allows applications to manage the device. The library supports both SNMP configuration and SNMP traps.



- **SNMP Enabled** – When checked, the library can be managed by computers listed in the SNMP Target IP Addresses field.
- **Community Name** – A string used to match the SNMP management station and library. It must be set to the same name on both the management station and the library. The default community name is *public*.
- **SNMP Targets** – List of configured SNMP targets.

To add an SNMP target or edit information for an SNMP target:

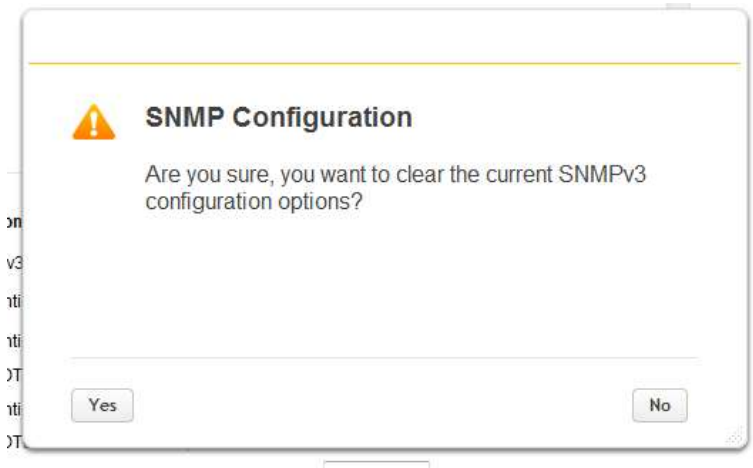
1) Click **Edit** for the appropriate SNMP target. When adding an SNMP target, click **Edit** next to a target without an IP/Hostname.
2) Enter the target IP address or hostname
3) Enter the port.
4) Select the SNMP version.
5) Enter the SNMP community string for the target.
6) Click **Submit**.

To delete an SNMP target:

1) Click **Delete** for the target to be deleted.
2) Click **Submit**.

To clear SNMPv3 Options:

1) Click **Clear SNMPv3 options**
2) To confirm that you want to clear the SNMPv3 Options, click **Yes**.



Configuring Event Notification Parameters

From the **Configuration > Network Management > SMTP** screen you can enable SMTP (Simple Mail Transfer Protocol) functionality and configure e-mail notification of library events. The library must have network access to an SMTP server.

- **SMTP Enabled** – Check to enable SMTP. When checked, the remaining configurations are active.
- **Notification Level** – The types of events for which the library should send e-mail
  - **Inactive** – No events are sent.
  - **Critical** – Only critical events are sent.
  - **+ Warnings** – Only critical and warning events are sent.
  - **+ Configuration** – Only critical, warning, and configuration events are sent.
  - **+ Information** – All events are sent.

- **SMTP Server** – Hostname or IP address of the SMTP server
- **Security** – Security protocol for accessing the SMTP server
    - **None**
    - **SSL => SSL/TLS**
    - **TLS = STARTTLS**
- **SMTP Port** – SMTP server port. The default port for the selected protocol will be selected. You can choose one of the default ports or configure a custom port.
- **To Email Address** – The address to receive the reported events (for example firstname.lastname@example.com). Only one email address can be configured.
- **Mailer Name** – Name of the sender of the e-mail
- **Email Subject** – Subject line for the e-mail message
- **Emailer Address** – Return address to use for the e-mail message
- **Authentication Required** – When checked, a username and password are required to access the SMTP server.
- **Username** – User account for logging into the SMTP server when authentication is required
- **Password** – Password associated with the Username when authentication is required

Configuring Remote Logging

Use the **Configuration > Network Management > Remote Logging (rsyslog)** screen to enable and configure Remote Logging.

- **Remote Logging Enabled** – When checked, the library will start forwarding log messages in a selected IP Network.
- **Notification Level** – With this field you can select the notification level.
    - **Inactive** – No events are sent.
    - **Critical** – Only critical events are sent.
    - **+ Warnings** – Only critical and warning events are sent.
    - **+ Configuration** – Only critical, warning, and configuration events are sent.
    - **+ Information** – All events are sent.
- **Remote Logging Server** – Hostname or IP address of the Remote Logging server
- **Remote Logging Port** – Select between Default Remote Logging Port or Custom Port
- **Transport Protocol** – With this field you can select the Transport Protocol (UDP, TCP).

Configuring Library Partitions

The library has a flexible partitioning scheme with a few key constraints:

- SymplyPRO XTL 8 does not support partitioning.
- Each partition must have at least one tape drive. One drive in each partition will host the library LUN for the partition.
- The maximum number of partitions is 2
- Mailslots must be enabled for the library before they can be allocated to a partition.

  A partition does not need to have a mailslot. If a partition does not have a mailslot, the magazine must be accessed to import or export cartridges. Opening a magazine takes the library offline.

  Although the mailslot magazine is shared between partitions, the mailslot elements are assigned individually to partitions. The Wizards guide you through the partition configuration process. The wizards are only accessible from the RMI.

Partitions Wizards

- **Basic Partition Wizard** – You specify the number of partitions, and the wizard removes the current partition configuration and assigns the drives and storage slots as evenly as possible to the partitions. Any extra drives or slots are assigned to the first partition.

  Use the Basic Partition Wizard to configure partitions that will have similar resources or to configure the number of barcode characters to report to the host application and whether to report them from the left or right end of the label for a library with a single partition.

- **Expert Partition Wizard** – You add or remove partitions from the current partitions configuration and then edit each partition configuration to add or remove library resources.

  Use the Expert Partition Wizard to configure partitions that will have different resources or to adjust resource assignments for existing partitions or those created with the Basic Partition Wizard.

	**CAUTION**	The library will go offline while partitions are being configured. Ensure that all host operations are idle before running a partition wizard.

Using the Basic Partition Wizard

1) Click **Configuration** > **Basic Wizard** to start the wizard.
2) The **Information** screen displays the existing partitions, which will be deleted by the wizard.
3) Click **Proceed** and then click **Next**.
4) The **Create Partition Scheme** screen displays the number of slots, mailslots, tape drives, and maximum available partitions for the library.



NOTE If you want to enable or disable the mailslots, **Cancel** out of the wizard and update the mailslot configuration before configuring partitioning.

5) Select the number of partitions.
6) Select the number of barcode characters reported to the host application. This option provides interchange compatibility with libraries with more limited barcode reading capabilities. The maximum length is 16 and the default is 8. This configuration will apply to all partitions.



NOTE The industry standard length for LTO barcode labels is eight characters. Barcode labels longer than eight characters might scan incorrectly, particularly if they are not high-quality labels.

7) Select whether to report the barcode characters from the left or right end of the barcode label to the host application when reporting fewer than the maximum number of characters. For example, when reporting only six characters of the barcode label 12345678, if alignment is left, the device will report 123456. If alignment is right, the device will report 345678. The default is left. Click Next.
8) The **Finish Configuration** screen displays the proposed allocation of library resources into partitions.

- To update the configuration, click **Back**.
- To have the wizard configure partition as shown, click **Finish**.
- After the wizard reconfigures the partition, the library will come online automatically.
- To exit the wizard, click **Cancel** or **Exit**.



TIP You can use the Expert Partition Wizard to adjust the allocation of resources after creating the partitions with the Basic Partition Wizard.

Using the Expert Partition Wizard

Click **Configuration > Expert Wizard** to start the wizard. The **Create Partition Scheme** screen lists the current partitions, if any, and the free resources. Use the wizard to configure one partition at a time.

	NOTE	If you want to enable or disable the mailslots, **Cancel** out of the wizard and update the mailslot configuration before configuring partitioning.

1) To add a partition, click **Add** and then click **Next**.

	NOTE	The **Add** button will only be active if there are available resources. If there are no available resources, either edit a partition and release resources from it or remove a partition that contains extra resources.

2) Enter a name for the partition.
3) Select the number of barcode characters reported to the host application. This option provides interchange compatibility with libraries with more limited barcode reading capabilities. The maximum length is 16 and the default is 8. This configuration will apply to all partitions.

	NOTE	The industry standard length for LTO barcode labels is eight characters. Barcode labels longer than eight characters might scan incorrectly, particularly if they are not high-quality labels.

4) Select whether to report the barcode characters from the left or right end of the barcode label to the host application when reporting fewer than the maximum number of characters. For example, when reporting only six characters of the barcode label 12345678, if alignment is left, the device will report 123456. If alignment is right, the device will report 345678. The default is left. Click **Next**.
5) In the **Assign Storage Slots** screen, use the >> and << buttons to assign slots to the new partition and then click **Next**.
6) In the **Assign Mail Slots** screen, use the >> and << buttons to assign mailslots to the new partition and then click **Next**.
7) Individual mailslot elements cannot be shared between partitions. Importing or exporting cartridges in a partition without an assigned mailslot will require magazine access, which will take the library offline.
8) In the **Assign Drives** screen, use the >> and << buttons to assign drives to the new partition and then click **Next**.
9) If the partition has multiple tape drives, select the drive that will host the SCSI communication for the partition and then click **Next**.
10) The lowest numbered drive in the partition is the default.
11) Verify the partition configuration and then click **Finish**.
12) After the wizard reconfigures the partition, the library will come online automatically.
13) To remove a partition:

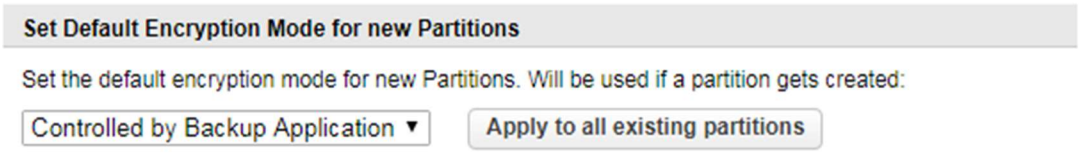
14) Select the partition, click Remove, and then click **Next**.
15) Verify that you want to remove the partition and then click **Finish**.
16) After the wizard removes the partition, the library will come online automatically.

Configuring Encryption

The **Configuration > Encryption** page provides several options to set encryption mode.

	NOTE	When changing certain configuration options, the library will go offline to hosts. Only perform these configuration changes when it is acceptable for the library to go offline.

To set the **Default Encryption Mode for new Partitions** select the encryption mode from the dropdown box.



Click the **Apply to all exiting partitions** button to set the selected encryption mode for all exiting partitions. Click the **Submit** button to activate the encryption modes.



Clicking the checkbox in section **General Settings** will allow the Administrator to enable and disable encryption during Expert Wizard

Section **Set Encryption Mode per Partition** allows you to select on a per-partition basis the encryption mode. Click the **Submit** button to activate the encryption modes.

KMIP Wizard

The library supports integration with encryption key management servers using the **KMIP standard**. These key management servers support sharing encryption keys with different libraries, which can be in different physical locations.

With the Key Management Interoperability Protocol (KMIP) Wizard you can configure use of KMIP key management servers with the library. Access to the wizard from the **Configuration > Encryption** menu is only available to the Security user and requires that the KMIP license has been added from the **Configuration > System > License Key Handling** screen.

For additional information on configuring KMIP servers for use with the library, see the KMIP server documentation.

Before running the wizard, verify that:

- The library configuration is complete, including defining all library partitions.
- The KMIP server is available on the network and has been configured for use with this library.

Using the KMIP Wizard

1) In the **Configuration** area, click **KMIP Wizard** in the **Configuration > Encryption** menu to start the wizard.
2) The **Wizard Information** screen displays information about the wizard. If the library configuration is complete and the KMIP server is available on the network, click **Next**.
3) The **Certificate Authority Information** screen displays prerequisites for using the KMIP certificate. When the prerequisites are met, click **Next**.
4) The **Certificate Authority Certificate Entry** screen displays instructions for obtaining the certificate for the KMIP server. Follow the instructions to copy the certificate from the management console. Paste the certificate into the wizard and then click **Next**.
5) The **Library Certificate Information** screen displays information about the next wizard steps. Click **Next**.
6) The **KMIP Client Configuration** screen provides options for two types of server authentication.
    a. If your KMIP server uses a client username and password for authentication, enter the username and password that were specified on the KMIP management console for the library.
    b. If your KMIP server uses *only* certificate passing for authentication, select **Enable KMIP Certificate-only authentication**. Only select this option if you are using a KMIP server that requires it and you do not have a client username and password.
7) Click **Next**.
8) The **Certificate Generation** screen displays the current library certificate, if one exists. To use the current certificate, select **Keep Current Certificate** and then click **Next**. To generate a new certificate, select **Generate New Certificate**. The wizard will generate and display a new library certificate. Click **Select Certificate** to copy the new certificate text and then click **Next**.
9) If you selected **Generate New Certificate**, the **Sign Library Certificate** screen displays the new certificate for the library. Sign the new library certificate with the certificate authority as a client certificate, paste the new KMIP certificate in the box, and then click **Next**.
10) In the **KMIP Server Configuration** screen, enter the IP address or fully-qualified hostname and port number for up to ten KMIP servers. To verify access to the KMIP servers, click **Connectivity Check**.

11) The **Setup Summary** screen displays the settings that were collected by the wizard. Verify that the settings are correct and that there are no errors in the **Done** column. If you need to modify any settings or fix any issues, either click **Back** to reach the applicable screen or **Cancel** out of the wizard to fix the issues and return later. If the settings are correct and there are no errors, click **Finish**.

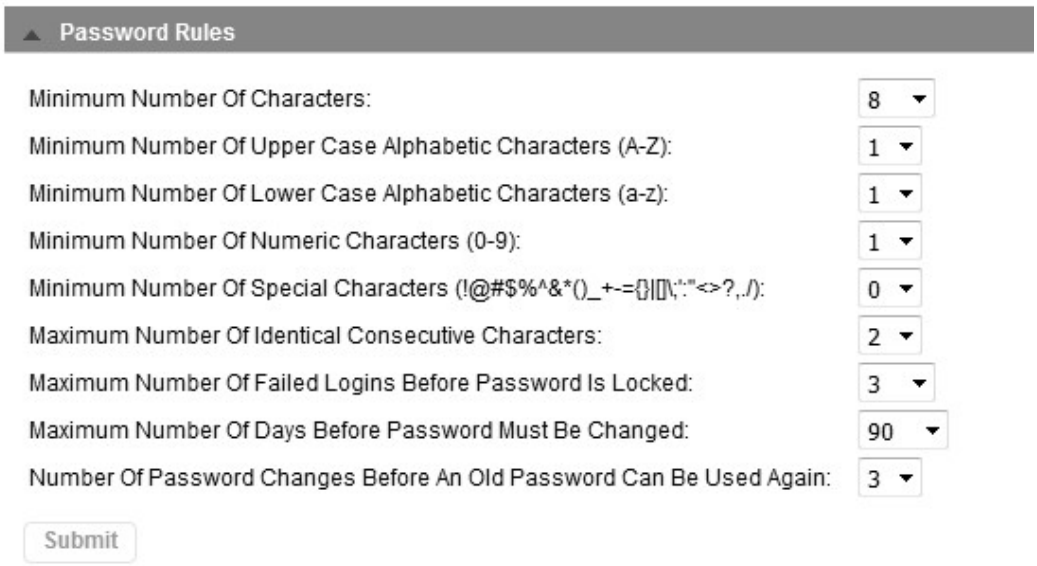
Configuring User Accounts

From the **Configuration > User Accounts** screen you can set or modify the following user account properties:

- User Account Settings
- Local User Accounts
- LDAP
- Kerberos

Configuring User Account Settings

From the page **Configuration > Configure User Accounts > Configure User Accounts Settings** you can configure the Password Rule settings.



- **Minimum Number Of Characters**
  Choose the minimum password length. The factory default value is 8. Possible range for this configuration option is from 8 to 20. The maximum password length is 20.
- **Minimum Number Of Upper Case Alphabetic Characters (A-Z)**
  Choose the minimum number of upper-case alphabetic characters. The factory default value is 1. Possible range for this configuration option is from 0 to 3.
- **Minimum Number Of Lower Case Alphabetic Characters (a-z)**
  Choose the minimum number of lower-case alphabetic characters. The factory default value is 1. Possible range for this configuration option is from 0 to 3.

- **Minimum Number Of Numeric Characters (0-9)**
  Choose the minimum number of numeric characters. The factory default value is 1. Possible range for this configuration option is from 0 to 3.
- **Minimum Number Of Special Characters** (!@#$%^&*()_+-={}|[]\;':" <>?,./)
  Choose the minimum number of special characters. The factory default value is 0. Possible range for this configuration option is from 0 to 3.
- **Maximum Number Of Identical Consecutive Characters**
  Choose the maximum number of identical consecutive characters. The factory default value is 2. Possible range for this configuration option is from Unlimited to 3.
- **Maximum Number Of Failed Logins Before Password Is Locked**
  Choose the maximum number of failed logins before the password is locked. The factory default value is 3. Possible range for this configuration option is from Unlimited to 10.



NOTE When a password is locked, the login cannot continue. Either the user must complete a valid login with an administrator account where the administrator can change a password or needs to get a temporary password for the administrator account.

- **Maximum Number Of Days Before Password Must Be Changed**
  Choose the maximum number of days before the password must be changed. In case the password is expired, you will be forced to change the password during the login. The factory default value is 90. Possible range for this configuration option is from Unlimited to 365.
- **Number of Password Changes Before An Old Password Can Be Used Again**
  Choose the amount of password changes to be done until a password can be used again. The factory default value is 3. Possible range for this configuration option is from 0 to 6.

Configuring Local User Accounts

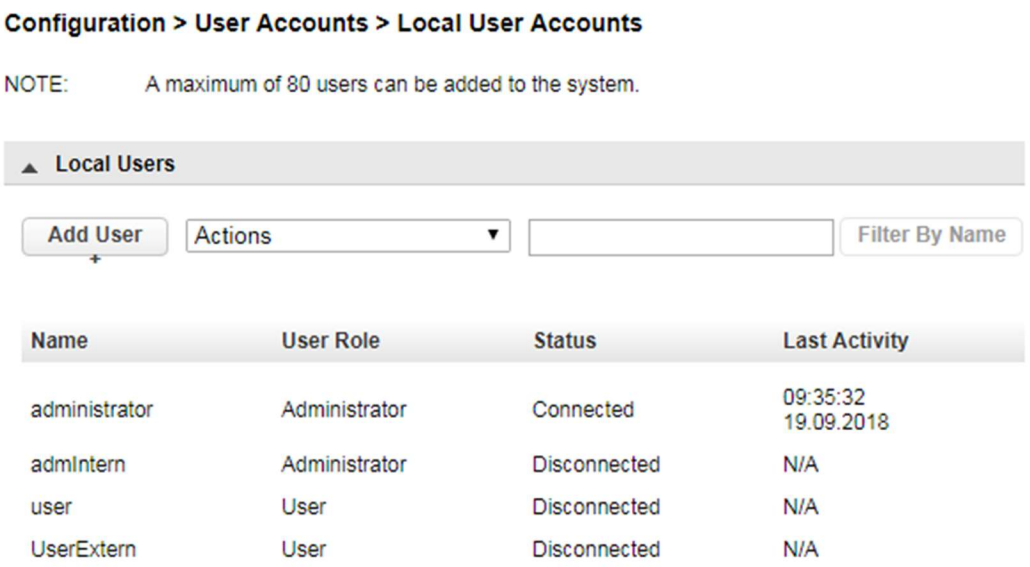
On the page **Configuration > User Accounts > Local User Accounts Settings** you can see the configured local users with access to the RMI.

By default, the library has four predefined user accounts: User, Administrator, Security and Service. When additional users are configured, the RMI login screens show the "custom users" along with the predefined users.

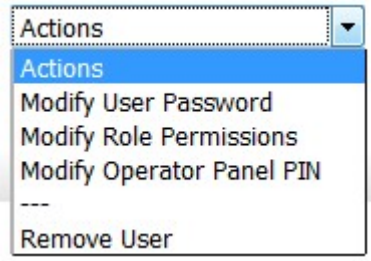
By pressing the Add User button you can add up to 80 users to the Local User Account list.

A dialog will be opened, and you must enter the username, select the user role and specify the a password according to the password rule settings.

The added user will be prompted to set a new password at the first login.



The Action dropdown list provides different actions to configure user accounts.



The table below lists the individual permission for each user role:

User Role	Permissions
User	no rights at all, not allowed to add/edit/delete any user
Administrator	allowed to add/edit/delete User and Administrator role allowed to change Role Permissions
Security	allowed to add/edit/delete Security role allowed to change Role Permissions
Service	allowed to add/edit/delete Security role allowed to change Role Permissions

Modify User Password

This action is only active if user is selected. Selecting this action will open a dialog where the Username and User Password can be changed. Please note that the name for default local user (user, administrator, service, security) are not changeable.

Modify Role Permissions

This action is permanent active. In the dialog you can allow Mailslot and/or Magazine access for the User Role.

Modify Operator Panel PIN

This action is permanent active. In the dialog you must select the user role first and then enter the new OCP PIN.

Remove User

This action is only active if user is selected. It is only valid for user which were previously added to the list. Default local user cannot be removed from the list

Configuring 2FA

In the context window "**Modify User Password** " it is possible to enable or disable a multi factor authentication method for each user.

The SymplyPRO XTL 8 and XTL 24 Gen2 tape library supports user login by Two Factor authentication.

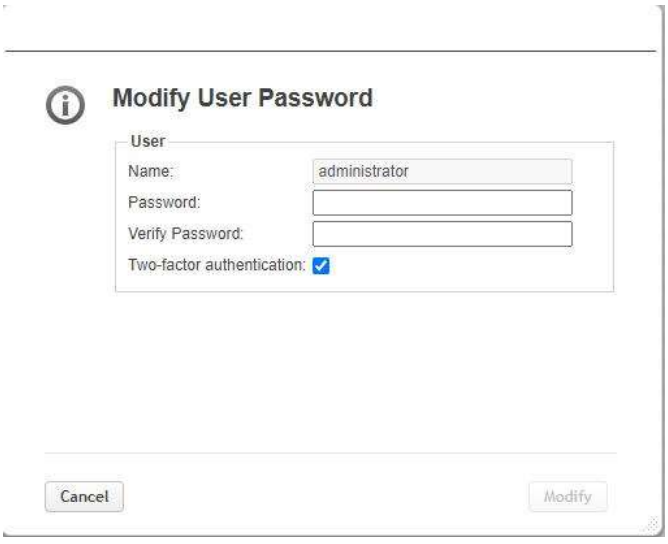
2FA Notes:

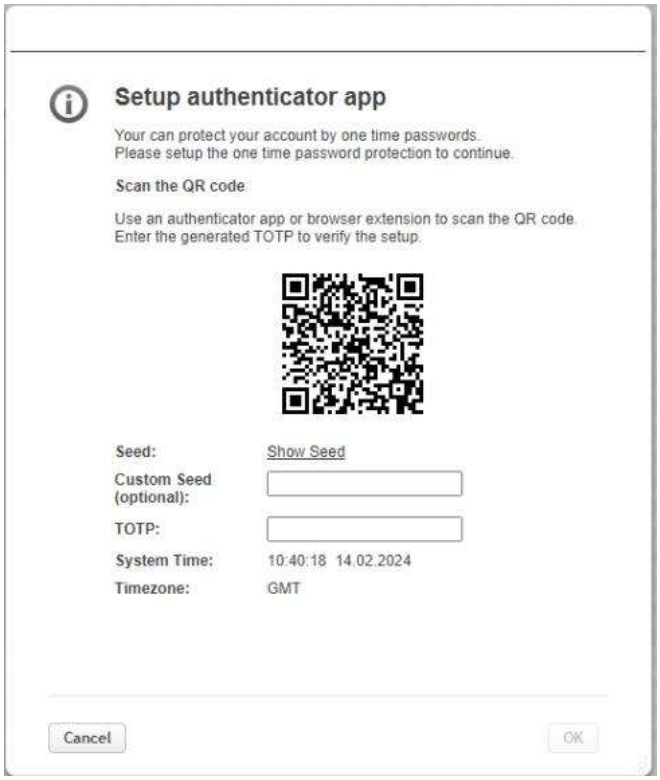
- NTP must be active to set 2FA for a user.
- NTP cannot be disabled if there are active 2FA users.
- Downgrade of Library FW to a level before 2FA was supported will be suppressed if any user has 2FA activated.
- Any authenticator app that supports TOTP with SHA1 can be used (e.g. Google Authenticator, Duo, Win Auth, etc.)
- Admins who want to configure 2FA for other users are obliged to have 2FA active themselves.

Enabling 2FA for the current logged in user will trigger a setup of 2FA directly on the active Session.

During this process the user can setup TOTP using the seed generated by the system or by providing a custom seed.

If these steps are successful, the TOTP will be set to active for that user:





This QR code can be scanned with an authenticator app to generate the TOTP, by clicking "**Show Seed**" the internal Seed (Key) can be displayed to put it manually to the app.

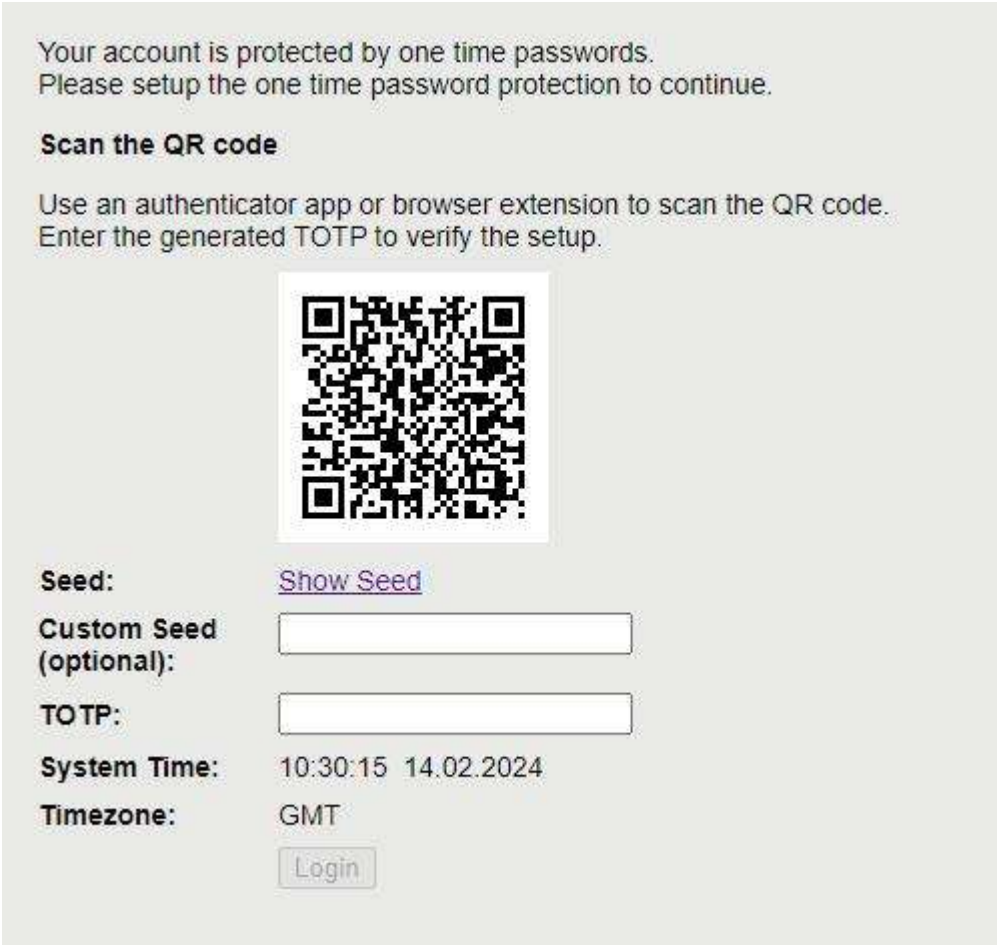
If custom seed is provided, that one will be used to validate the TOTP against and if valid store to DB.



Setting 2FA for another user or by adding a new user will set the TOTP state to "**Setup**" this will trigger the user to setup the TOTP (2FA) on his next valid login:



TOTP was set for another user will require that user to setup Two-step verification at his next login:



After successful setup the TOTP is required for each login:



If TOTP gets locked it will show a Recovery TOTP on the OCP to reset the TOTP settings for that user:



The OCP recovery window is only displayed for a limited time.



After recovering the account using the OCP recovery method the user is required to setup Two-step verification again.

Configuring LDAP

On the **Configuration > User Accounts > LDAP** page you can configure LDAP Servers and Users using for login on the RMI.

By default, the library has four predefined user accounts: User, Administrator, Security and Service. When LDAP servers and users are configured, the RMI login screens show the LDAP users along with the predefined users.

Each LDAP user is assigned to a role, based on the predefined user roles, and this role determines the access level for the LDAP user.



Using LDAP does not disable the predefined user accounts. For library security, ensure that the password for the predefined administrator user account is always set.

Setting the administrator password is required for any user with administrator role to log in from the RMI.



LDAP server configuration is dependent on the company's IT environment and security model. See your IT administrator for the settings for your environment. Before the wizard is used, you must know:

- IP address and port for the primary and backup LDAP servers
- User CN (Common Name) for the user who has access to the LDAP server
- User DN (Distinguished Name). This is the DN in which the User CN is located.
- Base DN. Parameters needed to search for potential library users in the LDAP server. For example, `OU=Users,OU=RW,DC=libgroup,DC=local`.
- Attribute Mapping, Username. For most Windows Active Directory environments, the **Username** field under **Attribute Mapping** should bet set to **sAMAccountName**.
- If SSL is required for the LDAP server. This field is likely required for newer versions of LDAP servers.

1) Navigate to the **Configuration > User Accounts > LDAP** page.
2) If not already listed, add your LDAP servers.
    a. In the **LDAP Servers** area click **Add Server**.
    The RMI displays the **Add Server** dialog.
    b. Enter all the requested LDAP configuration settings in the Primary Server area.

    See your LDAP server documentation or local LDAP administrator for the preferred values for the various LDAP configuration settings, such as the port number and distinguished names.

        i. **Host** - IP address for the LDAP server
        ii. **Port** - The default is 389 (636 with SSL). Port 3268 (3269 with SSL) when Base DN pointed to the global catalogue.
        iii. **User CN** (Common Name) - The LDAP user of the person or group that is the library administrator. Many environments use the format "Surname, Name" or the email address for a group of library administrators.
        iv. **User DN** - This is the DN where the User CN is included. For example: `DC=Examplegroup,DC=local`
        v. **Password** - LDAP password of the User CN. This might be the User CN's Windows password or an environment-specific password.
        vi. **Use SSL** - If SSL is required by your organization, select **Use SSL** and then paste the appropriate CA certificate.
    c. Enter the **Secondary/Backup Server** host address and port number.
    d. Enter the **Distinguished Name** and **Attribute Mapping** parameters.

        i. **Base DN** - The LDAP parameters for the LDAP accounts for potential library users. For example: `OU=lnternal,OU=Users,OU=RW,DC=examplegroup,DC=local`
    e. Click **Test Connection** to verify the configuration.
    f. When the library successfully connects to the LDAP server, click **OK**.
3) In the **LDAP User** area, click **Add User**.

    The RMI displays the **Add User** dialog.

4) Click **Query LDAP Servers** to see a list of available users.
5) Select the username and then assign the user a role (User, Administrator, Security or Service). Security user role can only be assigned by another security user. The other roles can be assigned by a user having the administrator role. Click **OK.**

LDAP server settings can be modified after the server was added. Selecting a server from the server list and choose **Modify Server** from the LDAP Servers action menu, will open the **Modify Server** dialog.

Removing a server can be done by selecting the server which should be removed and choose **Remove Server** from the LDAP Servers action menu. This action must be confirmed. The LDAP users that are related to the removed server are automatically removed together with the server.

The user role of an LDAP user can be modified after the user has been added. This can be done by selecting the specific user and using the **Modify User** action from the LDAP User action menu.

Removing a user can be done by selecting the user which should be removed and choose **Remove User** from the LDAP Users action menu. This action must be confirmed.

Configuring Kerberos

On the **Configuration > User Accounts > Kerberos** page you can configure Kerberos Servers and Users using for login on the RMI.

By default, the library has four predefined user accounts: User, Administrator, Security and Service. When Kerberos servers and users are configured, the RMI login screens show the Kerberos users along with the predefined users.

Each Kerberos user is assigned to a role, based on the predefined user roles, and this role determines the access level for the Kerberos user.



NOTE

Using Kerberos does not disable the predefined user accounts. For library security, ensure that the password for the predefined administrator user account is always set.

Setting the administrator password is required for any user with administrator role to log in from the RMI.



NOTE

Kerberos server configuration is dependent on the company's IT environment and security model. See your IT administrator for the settings for your environment. Before adding a server, you will need to know:

- Realm
- Default Domain
- KDC (Key Distribution Center) address and port
- Admin Server address and port

Default Domain and Admin Server are not a required configuration option for Kerberos 5 servers.

1) Navigate to the **Configuration > User Accounts > Kerberos** page.
2) If not already listed, add your Kerberos servers.
    a. In the **Kerberos Servers** area click **Add Server**.

       The RMI displays the **Add Server** dialog.

    b. Enter all the requested Kerberos configuration settings in dialog.
       See your Kerberos server documentation or local Kerberos administrator for the preferred values for the various Kerberos configuration settings.
        i. **Realm** - This is your Kerberos realm, which is usually a domain name in upper case letters. For example, the machine foo.abc.com is in the ABC.COM Kerberos realm.
        ii. **Default Domain** - The default domain of the Kerberos server.
        iii. **KDC, Port** - The address and port of the key distribution centre.
        iv. **Admin Server, Port** - The address and port of the admin server.
    c. Click **Test Connection** to verify the configuration.
    d. When the library successfully connects to the Kerberos server, click **OK**.

3) In the **Kerberos Users** area, click **Add User**.

   The RMI displays the **Add User** dialog.

4) Enter all of the requested user settings in dialog.
    a. **Principal** - Enter the name of the Kerberos Principal in this field. The Principal name consists of several components separated using the "/" separator.
    b. **Realm** - This is your Kerberos realm. A drop-down list offers the realms of the previously configured Kerberos servers.
    c. **User Role** - Monitor, Superuser or Administrator. The other roles can be assigned by a user having the administrator role.
5) Click **OK** to add the user.

Kerberos server settings can be modified after the server was added. Selecting a server from the server list and choose **Modify Server** from the Kerberos Servers action menu, opens the **Modify Server** dialog.

Removing a server can be done by selecting the server which should be removed and choose **Remove Server** from the Kerberos Servers action menu. This action must be confirmed. The Kerberos users related to the removed server are automatically removed together with the server.

The user role of a Kerberos user can be modified after the user has been added. This can be done by selecting the specific user and using the **Modify User** action from the Kerberos Users action menu.

Removing a user can be done by selecting the user which should be removed and choose **Remove User** from the Kerberos Users action menu. This action must be confirmed.

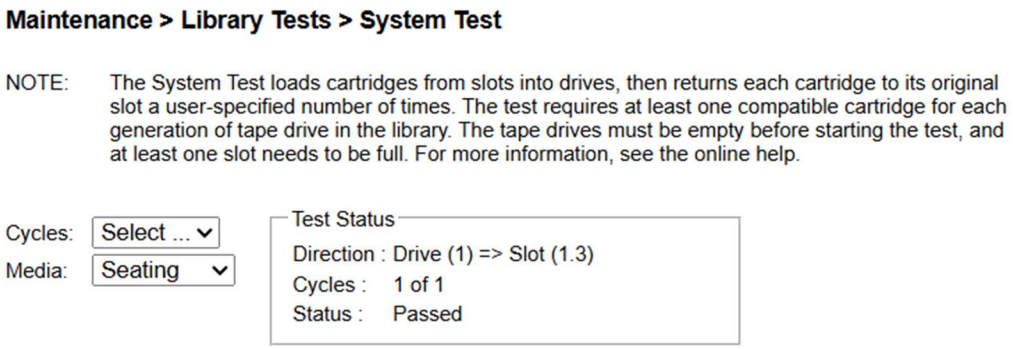
Maintaining the Library on the RMI

From the Home screen click or tap on **Maintenance** to access the library maintenance features.

System Test

The system test exercises overall library functionality by moving cartridges within the library.

- During each cycle the library will move a cartridge from a full slot to an empty drive and then return it to its original slot. You can select the number of cycles for the test. If the test is cancelled, the library will return the cartridge to its original slot.
- The library will not move cleaning cartridges during the test.
- The test operates over the whole library and does not consider partition configuration.
- During the test the library is offline.



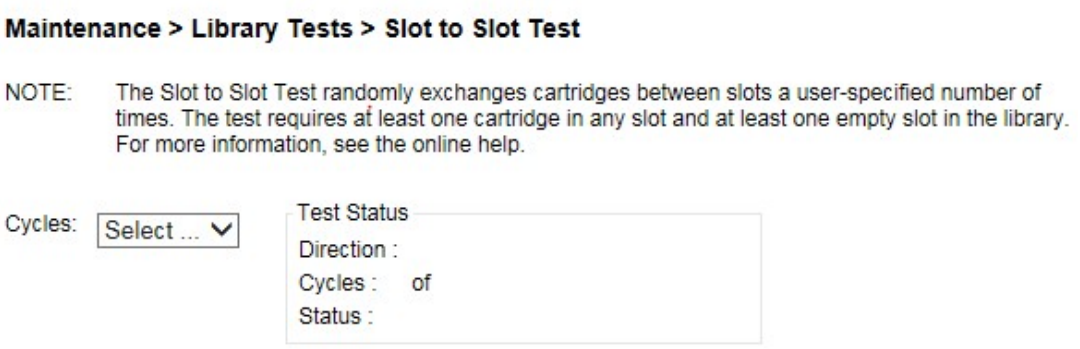
To run the system test, navigate to the **Maintenance > Library Tests > System Test** screen, select the number of cycles and then click **Start Test**.

Slot to Slot Test

The slot to slot test randomly exchanges cartridges between slots to verify that the library is operating correctly. At the end of the test the cartridges are NOT returned to their original slots. If a tape is moved to an incompatibly drive, the drive will reject the tape, as designed.

⚠	**CAUTION**	The test can move cartridges between partitions.

For service and diagnostics, use the robotic test.

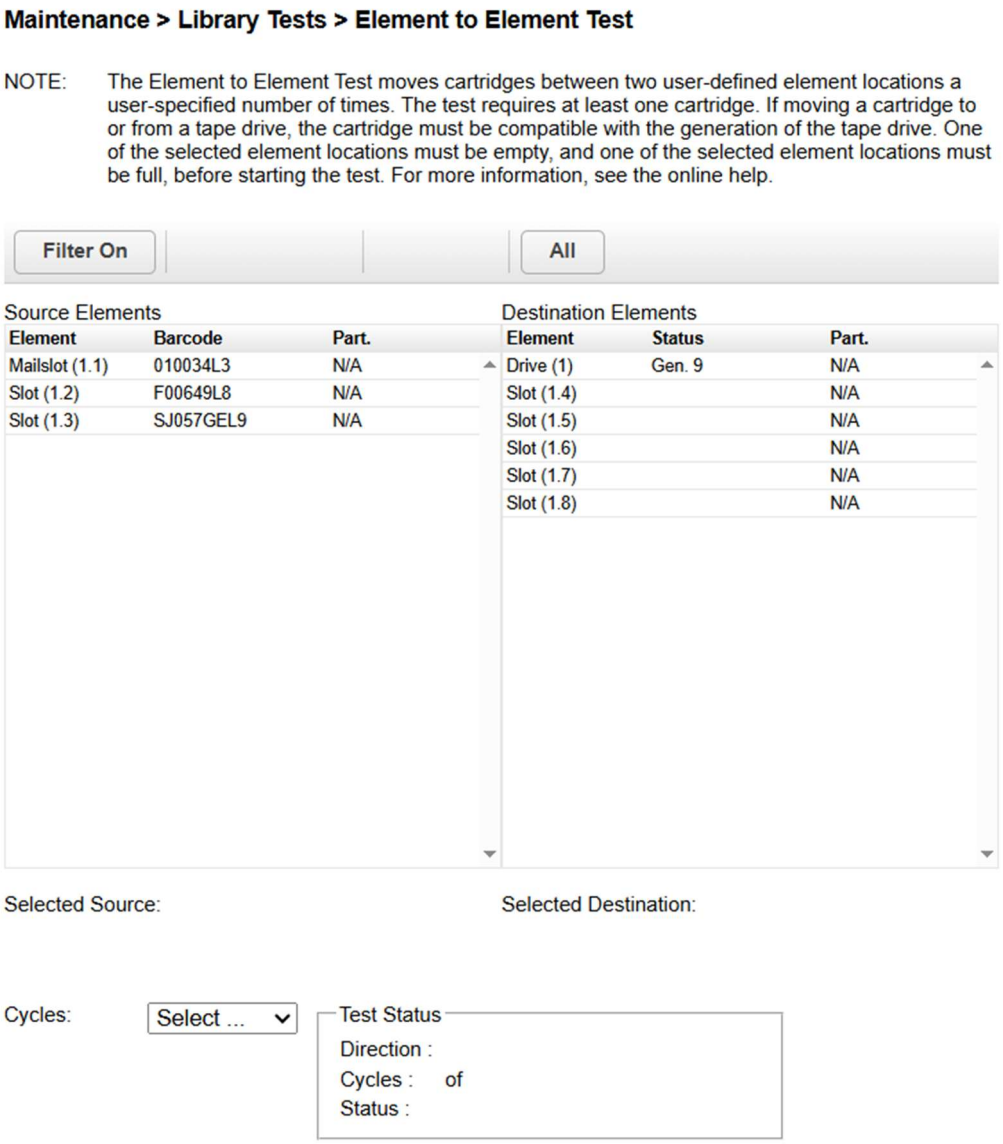


To run the slot to slot test, navigate to the **Maintenance > Library Tests > Slot to Slot Test** screen, select the number of cycles and click **Start Test**.

Element to Element Test

The element to element test moves a selected cartridge to a selected slot or tape drive, and then returns it to the original slot. You can select the number of times to move the selected cartridge to the destination location and back.

The element to element test is intended to show that the library is operating correctly. To diagnose problems with the robotic assembly or verify that it has been correctly replaced, use the robotic test.



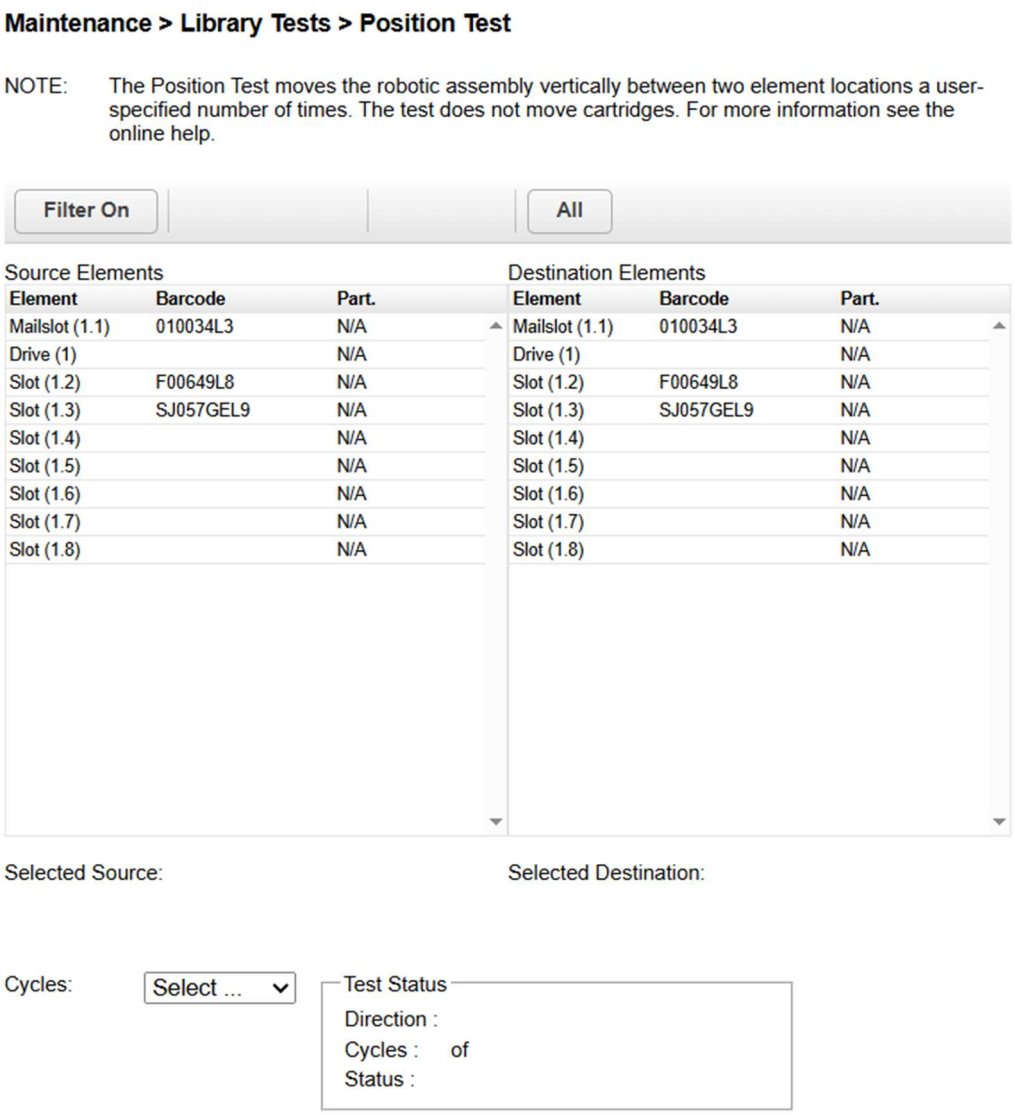
To run the element test:

1) Navigate to the **Maintenance > Library Tests > Element to Element Test** screen.
2) Select a cartridge from the **Source Elements** list.
3) To select from a subset of the cartridges:
    a. Click **Filter On**.
    b. Enter characters into the search box and then click **Search**.
4) The **Source Elements** list is updated to only include cartridges with a barcode label including the search characters.
5) Select a location from the **Destination Elements** list.
6) Select the number of cycles.
7) Click **Start Test**.

Position Test

The position test moves the robotic assembly vertically between two element locations. The test does not move cartridges. You can select the number of times to move the robotic assembly between two element positions.

The position test is intended to show that the vertical movement of the robotic assembly is operating correctly. To diagnose problems with the robotic assembly itself or verify that it has been correctly replaced, use the robotic test.

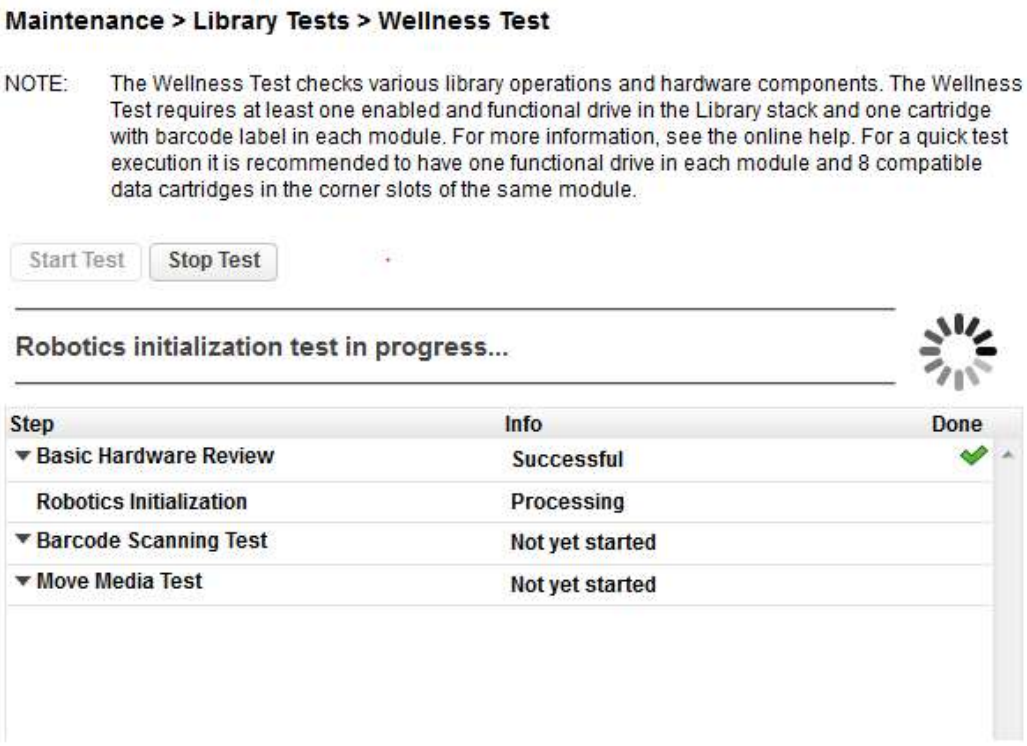


To run the position test:

1) Navigate to the **Maintenance > Library Tests > Position Test** screen.
2) Select a source location from the **Source Elements** list.
3) Select a destination location from the **Destination Elements** list.
4) Select the number of cycles.
5) Click **Start Test**.

Wellness Test

- The wellness test exercises a general health check on library functionality by running the following partial tests:
  - Basic Hardware Review
  - Robotics Initialization Test
  - Barcode Scanning Test
  - Move Media Test
- Running the test requires at least one enabled and functional drive and one cartridge with a barcode label in each module.
- After the test has been started the **Stop Test** button is active. Clicking the button will abort the wellness test but not before the current partial test has been completed.
- The test operates over the whole library and does not consider partition configuration.
- During the test the library is offline.
- The Info column notifies the user about the status and result of each partial test.

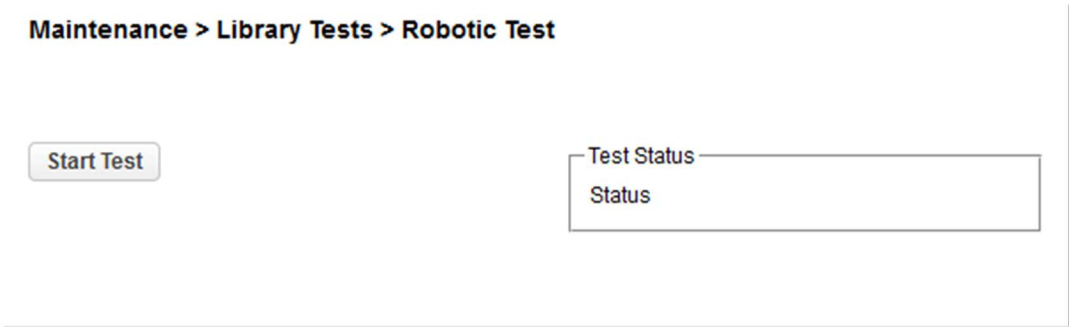


To run the Wellness test, navigate to the **Maintenance > Library Tests > Wellness Test** screen, and then click **Start Test**.

	NOTE	For quickest test execution it is recommended to have one functional drive in each module and 8 compatible data cartridges in the corner slots of the same module.

Robotic Test

The robotic test exercises all robotic assembly movements and sensors.

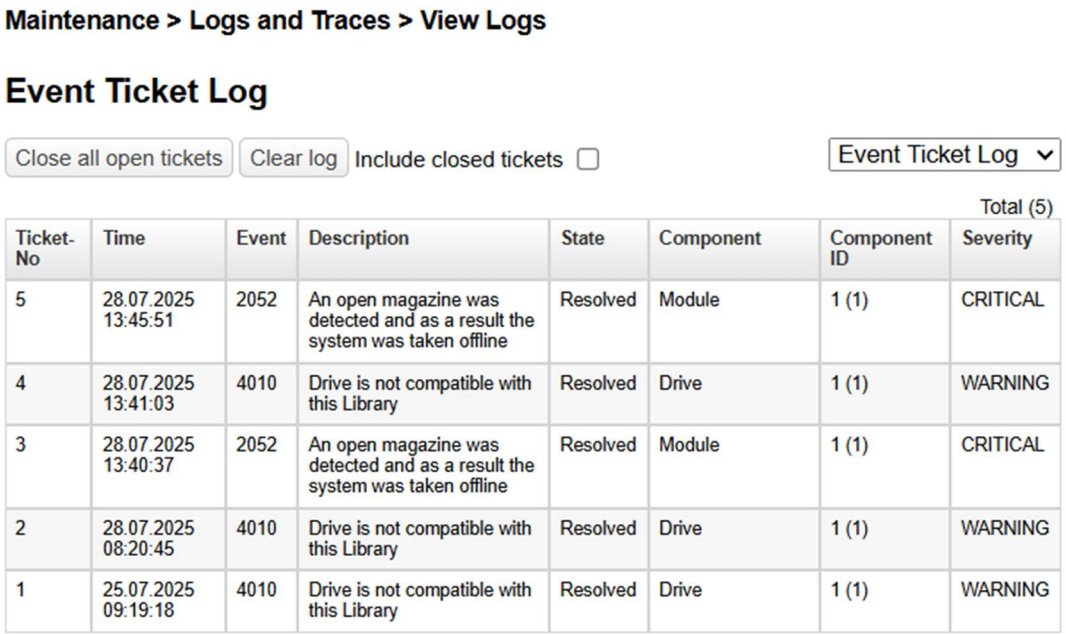


To run the robotic test, navigate to the **Maintenance > Library Tests > Robotic Test** screen, then click **Start Test**.

Viewing Log Files

To view the library log files, navigate to the **Maintenance > Logs and Traces > View Logs** screen and then select one of the logs. The available logs are:

- **Event Ticket Log** – Records library error and warning events
- **Information Log** – Records library information warnings
- **Configuration Log** – Records configuration changes



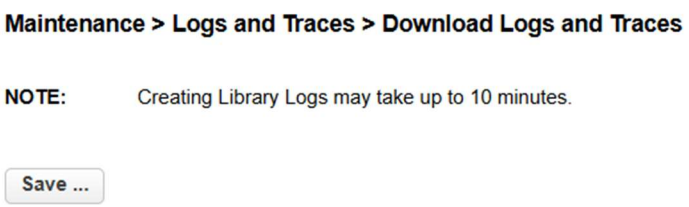
Ticket-No	Time	Event	Description	State	Component	Component ID	Severity
5	28.07.2025 13:45:51	2052	An open magazine was detected and as a result the system was taken offline	Resolved	Module	1 (1)	CRITICAL
4	28.07.2025 13:41:03	4010	Drive is not compatible with this Library	Resolved	Drive	1 (1)	WARNING
3	28.07.2025 13:40:37	2052	An open magazine was detected and as a result the system was taken offline	Resolved	Module	1 (1)	CRITICAL
2	28.07.2025 08:20:45	4010	Drive is not compatible with this Library	Resolved	Drive	1 (1)	WARNING
1	25.07.2025 09:19:18	4010	Drive is not compatible with this Library	Resolved	Drive	1 (1)	WARNING

The log entries are displayed in order of most recent to oldest. The log entries contain a date and time code, event code, severity, component identifier and event details. The format for the date and time is: *YY.MM.DD HH.MM.SS.ss*.

- YY.MM.DD – The date displayed as Year.Month.Day
- HH.MM.SS.ss – The time displayed as Hour.Minute.Second.Hundredths of a second

Downloading Log and Trace Files

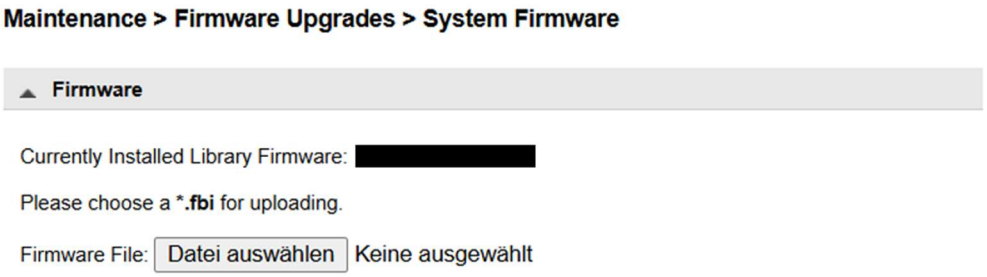
NOTE Users and Administrators should download support tickets instead of log and trace files because the support ticket will have complete information about each library event and is easier to read. See [`Downloading Support Tickets`].



To download the library log and trace files from the RMI, navigate to the **Maintenance > Logs and Traces > Download Logs and Traces** screen and then click **Save**.

Managing System Firmware

The firmware version currently installed on the library is displayed in the library status area on the Home page. You update the library firmware from the **Maintenance > Firmware Upgrades > System Firmware** screen.



To update library firmware from the RMI, click **Choose File** and select the firmware file from the local computer.

To update the library firmware from the OCP

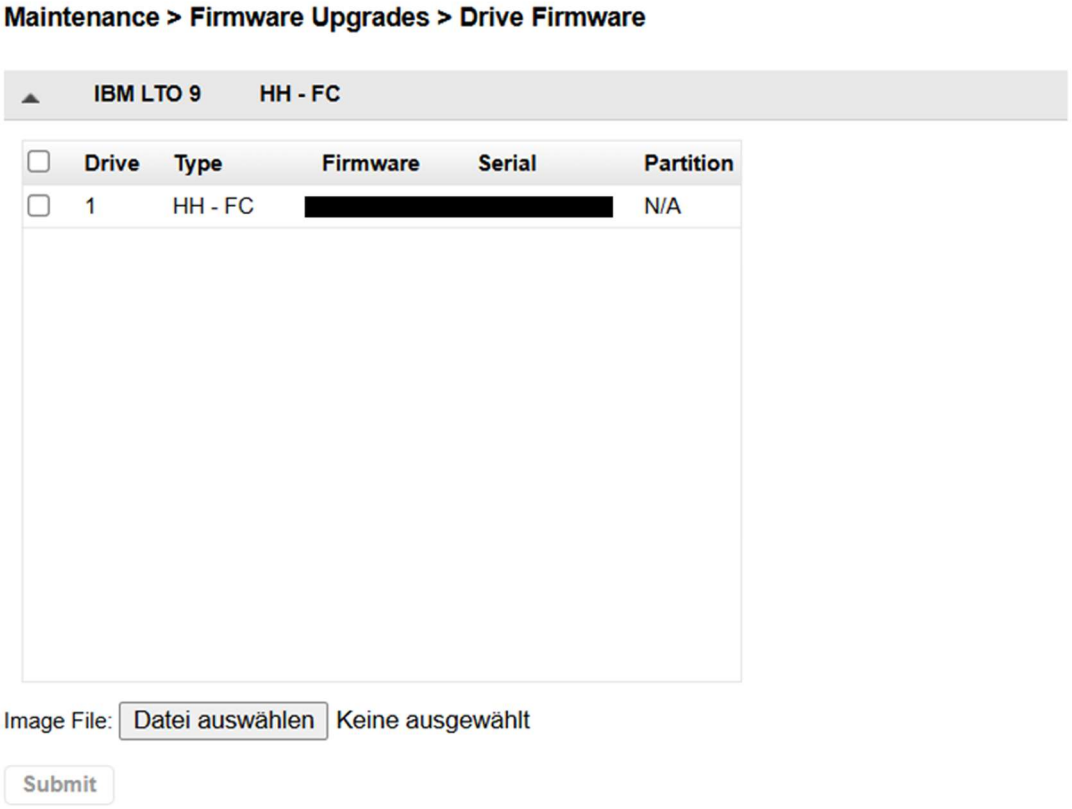
1) Copy the firmware file to the USB thumb drive.
2) Insert the USB thumb drive into the USB port at the back of the library.
3) The library detects the USB thumb drive.
4) Select the firmware file.
5) Click **Start Upgrade**.

When you update the library firmware, the library will also update the firmware of the expansion modules to a compatible version.

Managing Drive Firmware

Drive firmware can be updated on multiple drives of the same type at the same time. Drive firmware can be updated from the RMI. Each drive will only accept appropriate firmware.

To see the firmware version currently installed on the drives, navigate to the **Status > Drive Status** screen.

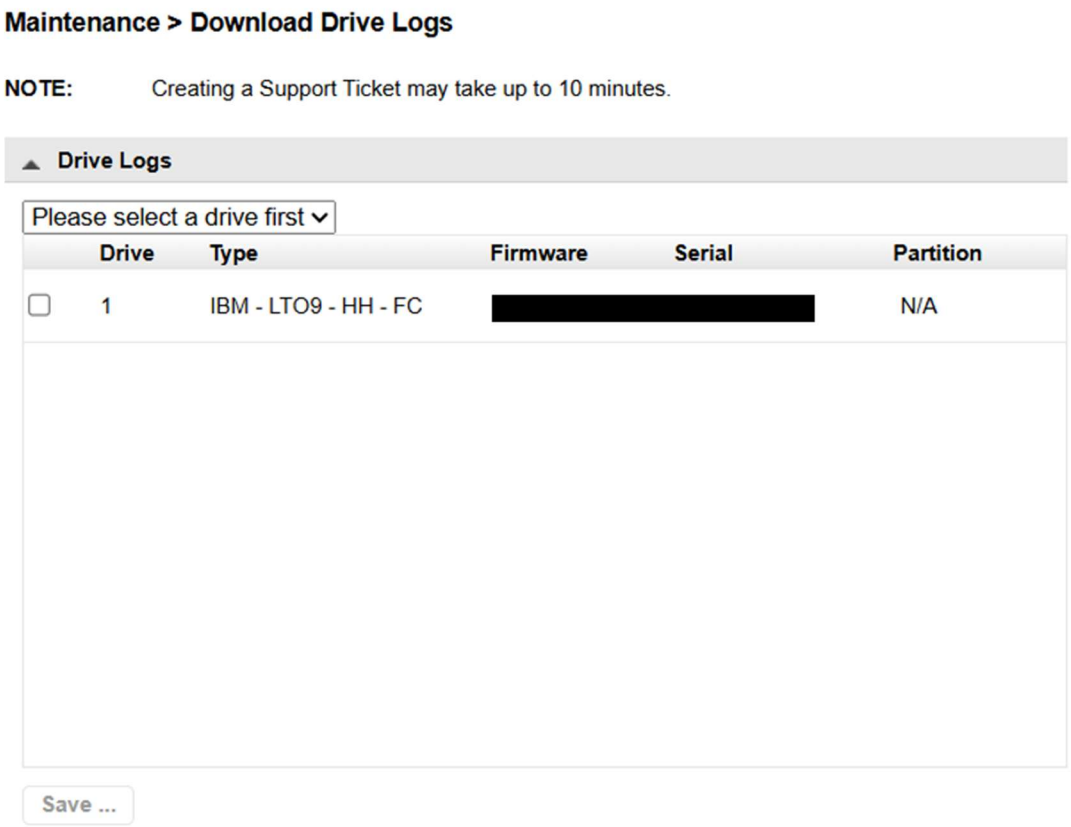


To update drive firmware from the RMI

1) Navigate to the **Maintenance > Software Upgrades > Drive Firmware** screen. The tape drives are organized by drive type.
2) Expand the appropriate drive type and select one or more of the tape drives.
3) Click **Choose File**, and then select the file from the local computer.
4) Click **Submit**.

Downloading Support Tickets

From the **Maintenance > Download Support Ticket** screen you can download a support ticket from the library or any of the tape drives.



To download a drive support ticket

1) Expand the **Drive Support Ticket List**, if necessary, by clicking the down arrow on the left side.
2) The drive list displays:
    a. **Drive** – The drive number. Drives are numbered starting with one from the physical bottom of the library to the top.
    b. **Type** – The drive form factor (half height or full height) and interface
    c. **Firmware** – The current drive firmware version
    d. **Serial** – The drive serial number
    e. **Unit** – The module containing the tape drive
    f. **Partition** – The logical library associated with the tape drive
3) Select the ticket to download.
    a. **Current Ticket** – Pulls and saves a new support ticket from the drive.
    b. **Last Unload Ticket** – Saves the ticket that was pulled automatically after the last cartridge was unloaded from the drive
4) Check the drive.
5) Click **Save**.

To download a library support ticket

1) Expand the Library Support Ticket area, if necessary, by clicking the down arrow on the left side.
2) Click **Save**.

To download a drive support ticket

1) Expand the **Library Support Ticket** list, if necessary, by clicking the down arrow on the left side.
2) Click **Save**.

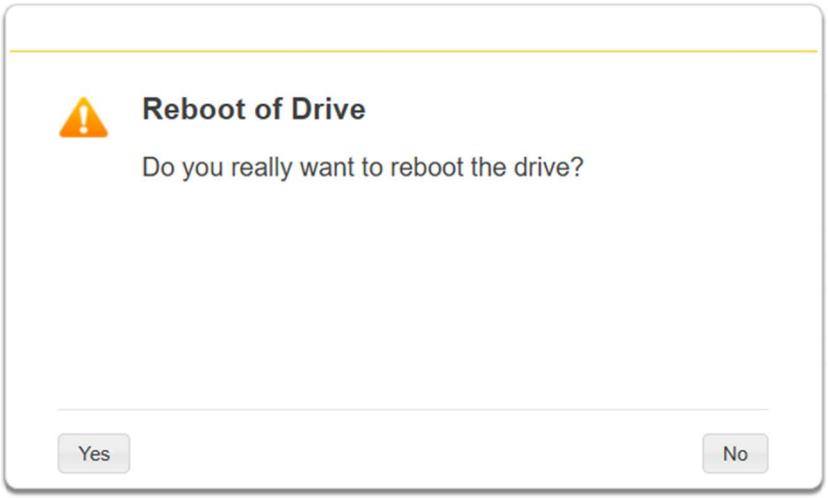
Rebooting the Library via RMI

To reboot the Library navigate to the **Maintenance > System Reboot** page and click the **Reboot** button.

Rebooting Drives via RMI

1) Select the drive you want to reboot.
2) Click Yes on the dialog popup to start the reboot process.
3) Only one drive can be selected for reboot.





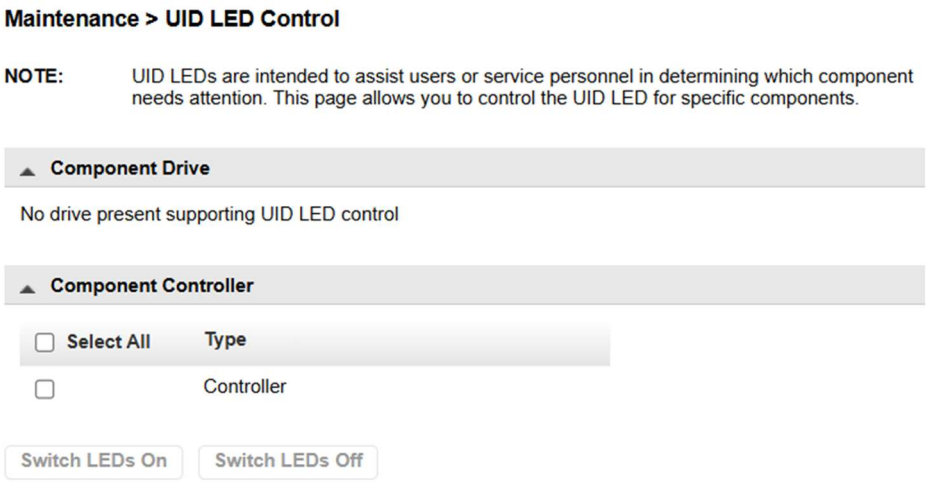
Controlling the UID LEDs

UID (Unit Identification) LED generally refers to blue LEDs on the tape library that assist users and service personnel in determining which component requires attention.

There are two groups of UID LEDs in the SymplyPRO XTL 8 and XTL 34 Gen2 tape libraries.

- **Base Library** (one LED per controller)
- **Power Supply**

Additionally, there is one UID LED on the Operator Control Panel OCP. Control of this LED is linked to the base controller UID LED (i.e. if the base controller is selected and its UID LED is switched on, the OCP UID LED will be switched on as well).



To select and switch on UID LEDs, navigate to the page **Maintenance > UID LED.**

1) Expand the **Component Drive** or **Component Module** list, if necessary, by clicking the down arrow on the left side.
2) Select the component where you want to switch on the UID LED.
3) Click the **Switch LEDs On** button

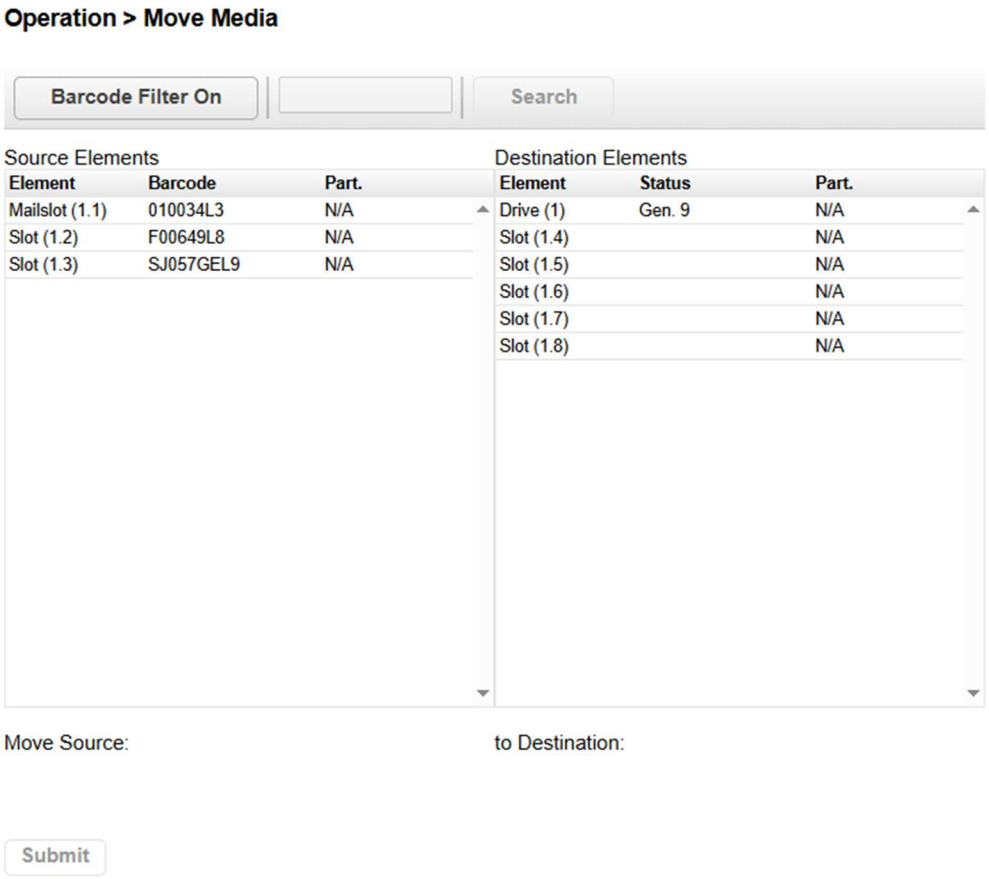
Run the same procedure if you want to switch off UID LEDs.

Operating the Library on the RMI

Click or tap the **Operations** button on the Home screen to access the operations features.

Moving Media via RMI

From the **Operation > Move Media** screen you can move a tape cartridge located in a source element to an available destination element within the same partition.



- **Source Elements** – Tape drives, enabled mailslots, and storage slots that contain a tape cartridge
- **Destination Elements** – Tape drives, enabled mailslots, and storage slots that do not contain a tape cartridge
  - Tape drives are listed at the top of each element list and listed in the order of their drive numbers.
  - Tape drives are numbered from the physical bottom of the library starting with Drive (1).
  - Slots are listed in the order of the slot numbers. Slots are numbered *m.s*, where *m* is the module number and *s* is the slot within the module.

Filtering Based on Barcode

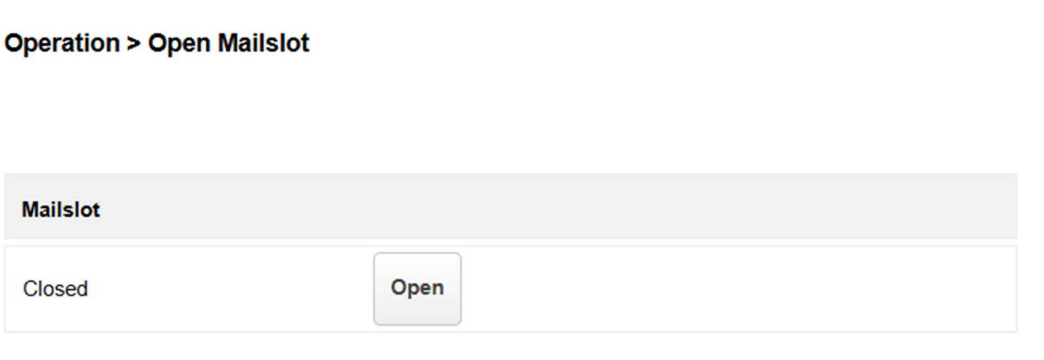
To see a subset of the cartridges in the library, enter some or all of the barcode label characters in the search area and click **Search**. The **Source Element** list updates to display only the cartridges with labels that include the characters in the search box.

To perform a different search or display all of the available cartridges, click **Barcode Filter Off**.

Moving a Cartridge

1) Select the cartridge from **Source Elements**.
2) Select the destination location from **Destination Elements**.
3) Click **Submit**.

From the **Operation > Open Mailslot** screen you can see the status and unlock any enabled mailslot in the library.



To open a mailslot, click **Open** for the appropriate mailslot. The library will release the lock. You can then pull the mailslot out of the library to access the mailslot.

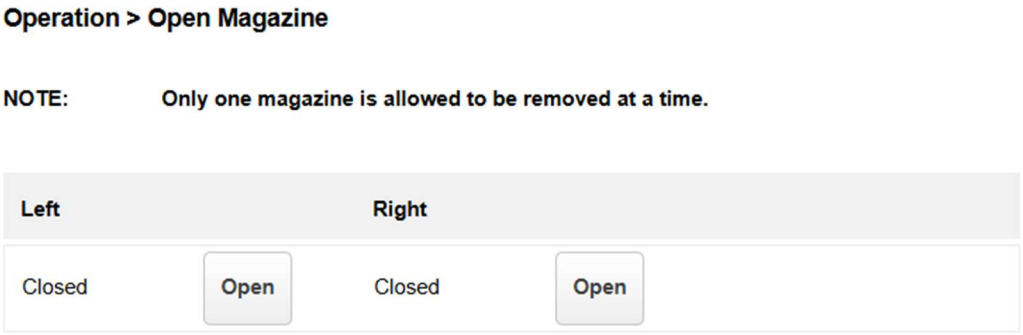
NOTE The mailslot will relock after 30 seconds.

The mailslot must be enabled before it can be opened. To enable a mailslot, see [Enabling or Disabling mailslots].

WARNING Hazardous moving parts exist inside this product. Do not insert tools or any portion of your body into the interior of the library while the mailslot is pulled out.

Opening a Magazine via RMI

From the **Operation > Open Magazine** screen you can unlock any magazine in the library.



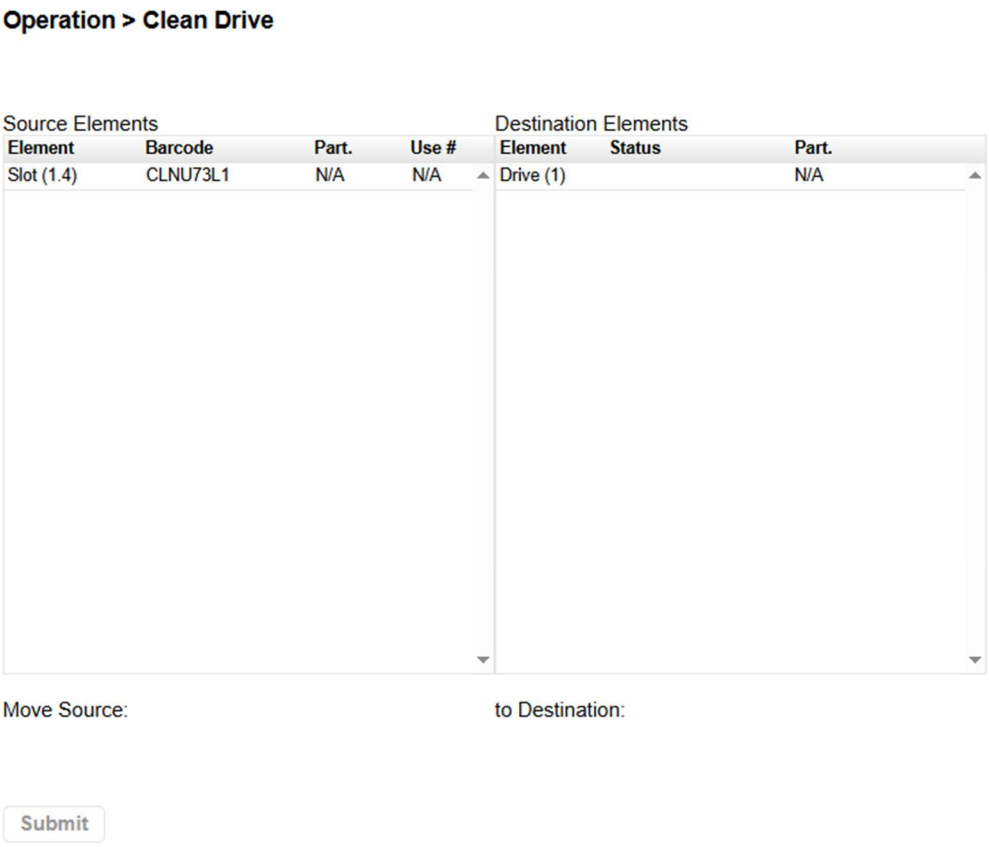
To unlock a magazine, click **Open** for the magazine. The library will release the lock. You can then pull the magazine out of the library to access the storage slots.

NOTE

- Opening a magazine will take the library off-line.
- The magazines will relock after 30 seconds.

Cleaning a Tape Drive via RMI

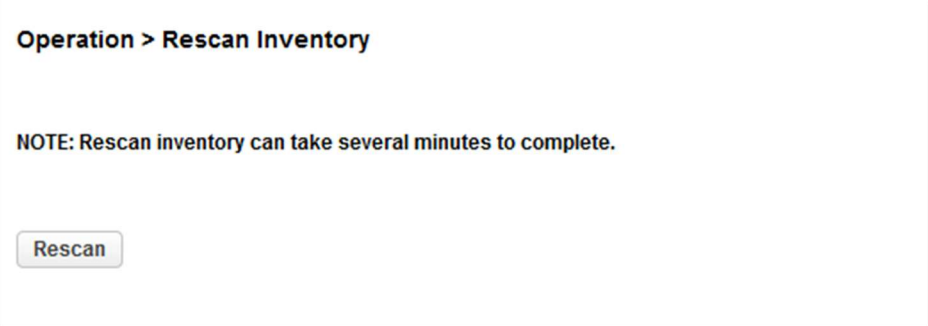
From the **Operation > Clean Drive** screen you can initiate a drive cleaning operation.



1) Select a cleaning cartridge from the **Source Elements** list. The library uses the barcode label to identify cleaning cartridges.
2) If no cleaning cartridges are available, load one into a mailslot or magazine slot.
3) Select the tape drive to be cleaned from the **Destination Elements** list.
4) Tape drives currently containing a cartridge are not listed. To clean a tape drive not listed, move the cartridge out of the drive.
5) Click **Submit**

Rescanning the Cartridge Inventory via RMI

To have the library rescan the cartridges, navigate to the **Operation > Rescan** screen and click **Rescan**. The library will change to Scanning status and will be unavailable to perform other operations until the scan is complete.

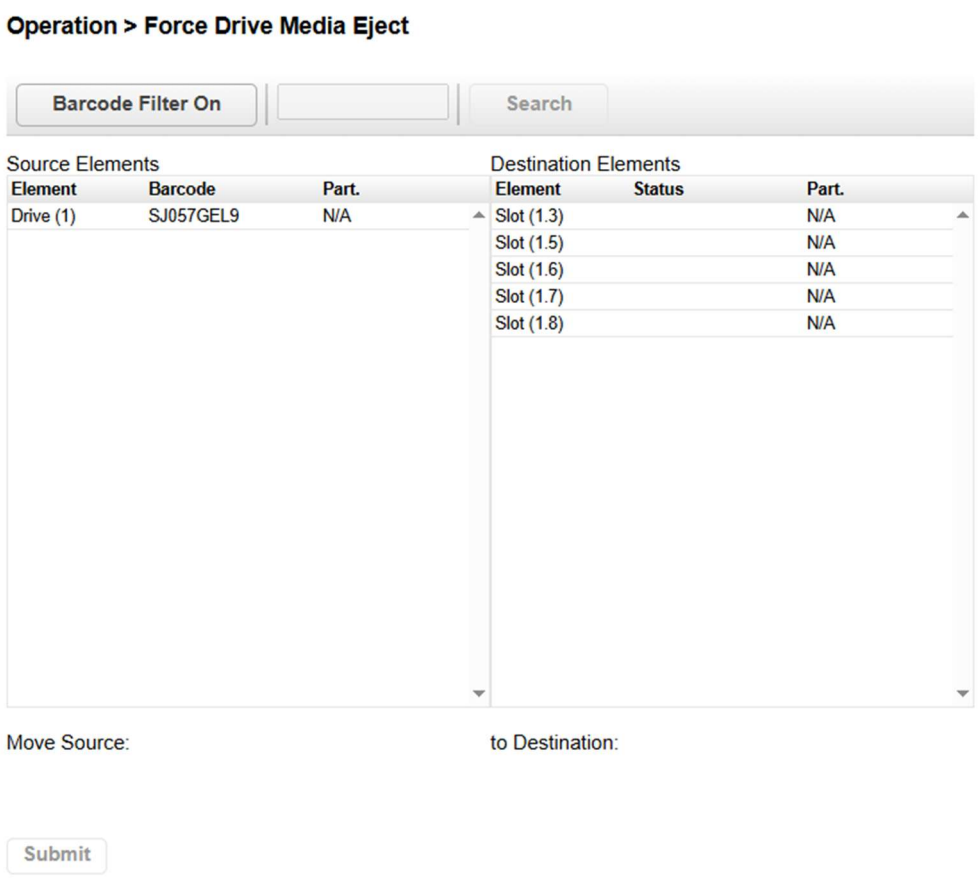


Forcing a Drive to Eject a Cartridge via RMI

The force drive media eject operation attempts to force the tape drive to eject the cartridge and place it into an open slot. Access to this feature requires the administrator password.

Before performing this option, it is recommended that you attempt to eject the tape using the backup software or library move media operation. While a drive is being force ejected, a window indicating the process is ongoing should appear. No operations will be available until the force eject completes.

	NOTE	If the drive has difficulty ejecting the cartridge, the media is possibly bad or damaged.



1) Navigate to the **Operation > Force Drive Media Eject** screen.
2) Select the drive in the **Source Elements** list.
3) Select the destination in the **Destination Elements** list.
4) Click **Submit**.

LTO-9 New Media Initialization Wizard

To use the Media Initialization Wizard (Optimization):

1) Navigate to the **Maintenance** > **LTO-9 New Media Initialization Wizard**.
2) Click **Start LTO-9 New Media Initialization Wizard**.
3) Click **Next** on the **Information** Screen.
4) Select the cartridge(s) you want to initialize and click the right arrow. If all the cartridges need to be initialized, click **Select All**, then click the right arrow.
    a. This will place the cartridges in the section to the right titled **Selected Cartridges**.
5) Click **Next**.
6) Select the drives to be used for initializing (optimizing) the media and click the right arrow. If all the drives are to be used, click **Select All**, then click the right arrow. This will place the drives in the section to the right titled **Selected Drives**.
7) Click **Next**.
8) Click **Finish** to complete the wizard and begin the media initialization (optimization) process on the selected tapes. The wizard screen will show the progress as the process completes. If you click **Exit**, you will leave the wizard, but the process will continue, and updates will be displayed on the **Maintenance** > **LTO-9 New Media**

Initialization Wizard page.



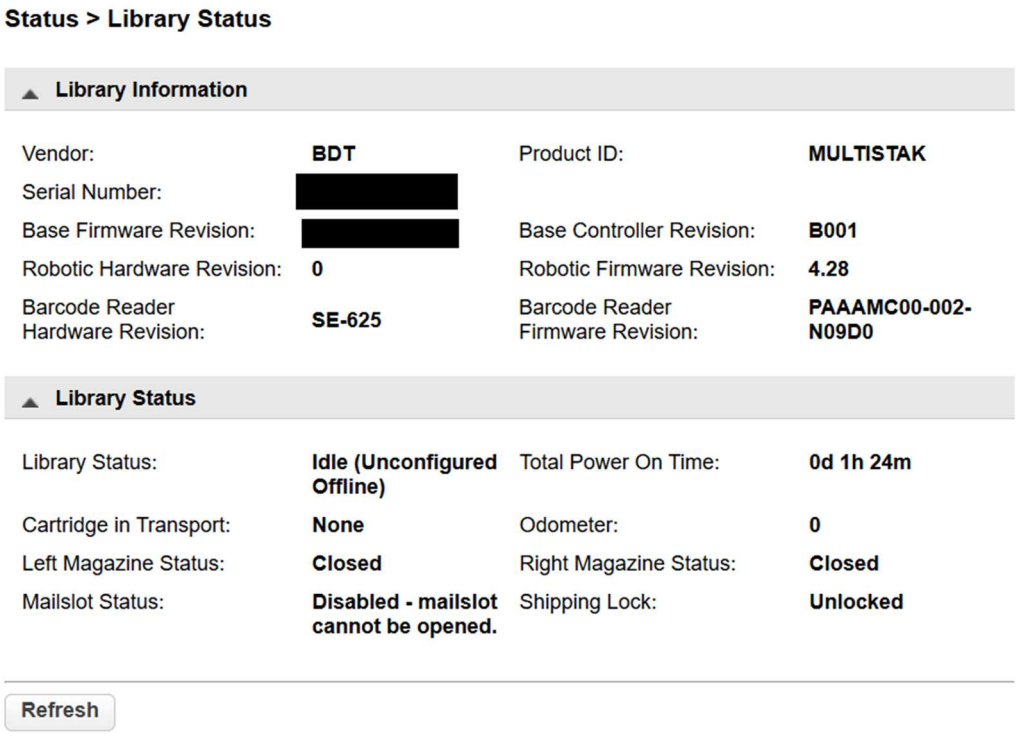
NOTE If needed, it is possible to abort the media initialization (optimization) process. It should be noted however, that once a tape is loaded in a drive, that media will complete its (optimization), which could take up to two hours. Once the currently loaded media completes initialization, the wizard will abort and not process any remaining media that was selected.

Viewing Status Information on the RMI

To access the status area, from the **Home screen**, click or tap **Status**.

Viewing Library and Module Status

Summary information and status is displayed in the top banner and the left side bar. For additional library module configuration and status information navigate to the **Status > Library Status** screen.



Library information:

- **Vendor**
- **Serial Number** – Library serial number
- **Base Firmware Revision** – Version of the currently installed library firmware
- **Robotic Hardware Revision**
- **Barcode Reader Hardware Revision**
- **Product ID**
- **Base Controller Revision**
- **Robotic Firmware Revision** – Version of the currently installed robotic assembly firmware. The robotic assembly firmware is bundled and installed with the library firmware.
- **Barcode** Reader Firmware Revision – Version of the currently installed barcode reader firmware. The barcode reader firmware is bundled and installed with the library firmware.

Library Status

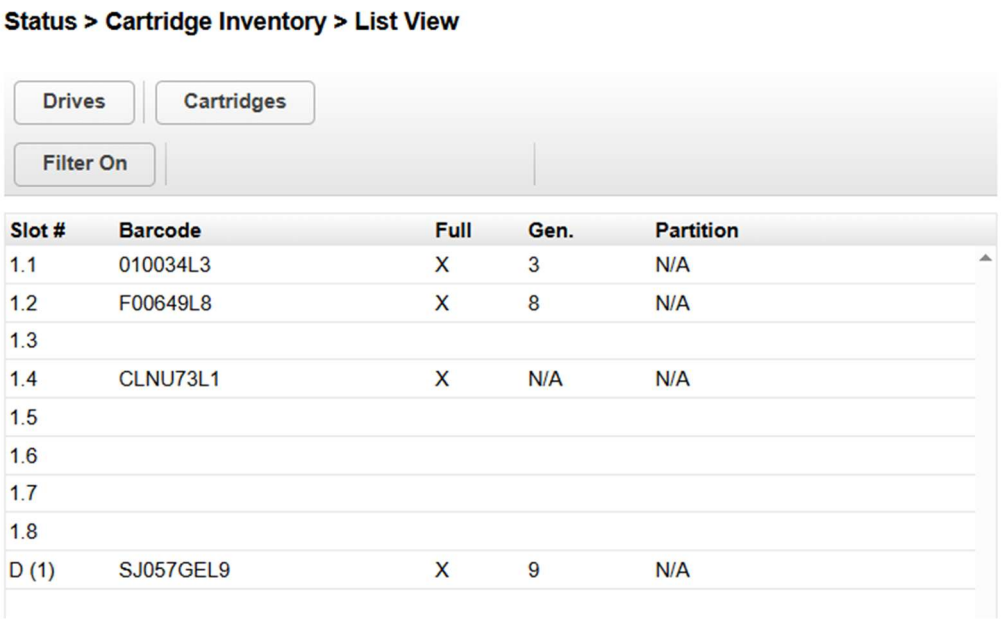
- **Library Status**
    - **Idle** – The library robotic is ready to perform an action.
    - **Moving** – The library robotic is moving a cartridge.
    - **Scanning** – The library robotic is performing an inventory of cartridges.
    - **Offline –** The library robotic has been taken off line by the library.
    - **Robotic Location –** Displays the module where the robotic is currently located
    - **Shipping Lock –** Indicates whether the robotic is unlocked or locked for shipment
- **Cartridge in Transport** – When applicable, displays the barcode label of the cartridge currently in the robotic assembly
- **Total Power On Time** – Total time that the Base Module has been powered on since it was manufactured
- **Odometer** – Robotic assembly move count
- **Left Magazine Status**
- **Right Magazine Status**
- **Mailslot Status**
- **Shipping Lock**

Using Inventory Lists

The inventory lists display each of the elements, such as slots and tape drives, with information about the cartridge stored in the element.

Cartridges stored in unused slots, which are not available for move operations, are greyed out and are not assigned to any partition

To see the elements organized by module, from **Status**, navigate to **Cartridge Inventory** → **List View**. To see the elements organized by logical library or partition, from **Status**, navigate to **Partition map** → **List View**.



In the Inventory List you can see:

- **Slot #** – The slot number in the form <module>.<slot>, where module is the module number and slot is the slot number
- **Barcode** – Barcode label
- **Full** – X if a cartridge is using the element
- **Gen** – LTO generation of the cartridge
- **Partition** – The partition number

Filtering by Barcode Label

To filter the list based on barcode label, enter characters in the filter box and then click **Search**.

1) Click **Filter On.**
   The search box is displayed.
2) Enter characters into the search box and then click **Search**.
   The characters can be anywhere in the barcode label. The search characters are not case sensitive. There are no wildcards.

   To disable filtering, click **Filter Off**.

Listing Just Drives or Cartridges

To limit the list to tape drives, click **Drives**.

To limit the list to cartridges, click **Cartridges**.

To see all elements, click **Partition** or **Slots**.

Viewing Elements by Group

When the list is grouped, you can expand or contract the list for each group by clicking the triangle next to the number in the first column. Grouping is enabled by default.

To disable grouping, click **Group Off**.

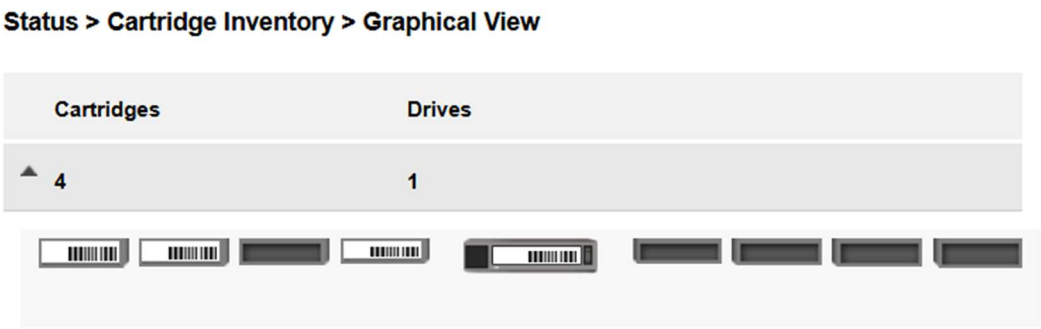
To enable grouping, click **Group On**.

Using Inventory Graphical View

The inventory graphical view displays each of the elements, such as slots and tape drives, with information about the cartridge stored in the element.

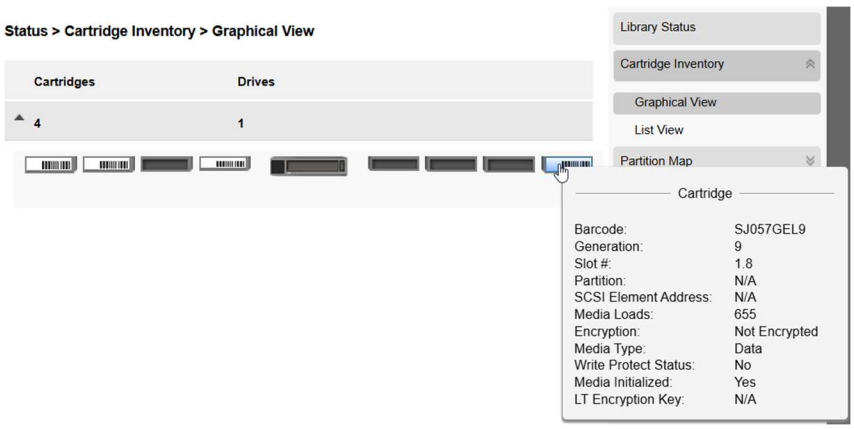
Unused slots, which are not available for move operations, are greyed out and marked with a cross. Cartridges stored in these slots are displayed in the same way as for regular slots.

To see the elements organized by module, from **Status**, navigate to **Cartridge Inventory** > **Graphical View**. To see the elements organized by logical library or partition, from **Status**, navigate to **Partition Map** > **Graphical View**.

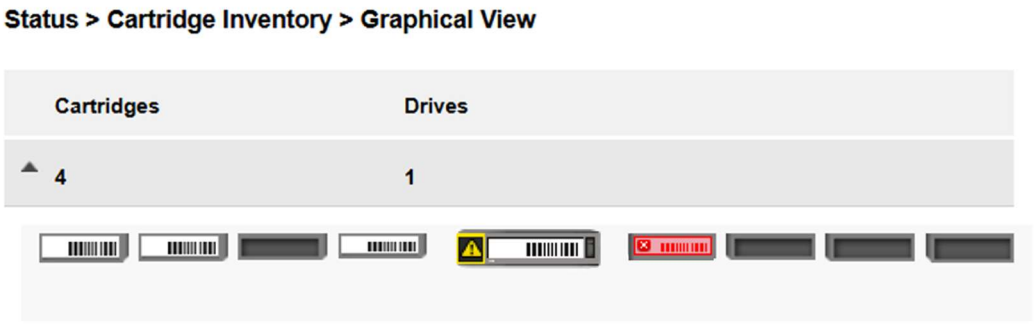


Moving the mouse over drive or cartridge will display additional information:

- **Drive** – LTO generation of drive and format (Full Height or Half Height)
- **Drive #** - The drive number
- **Serial #** - Serial number of the drive
- **Slot #** – The slot number
- **Barcode** – Barcode data on label
- **Generation** – LTO generation of cartridge
- **Partition** – The partition number
- **Media Loads** – The number of media loads
- **Encryption** – Indicates whether data on this media is encrypted or not encrypted
- **Media Type** – Indicates whether this media is a data or a cleaning cartridge



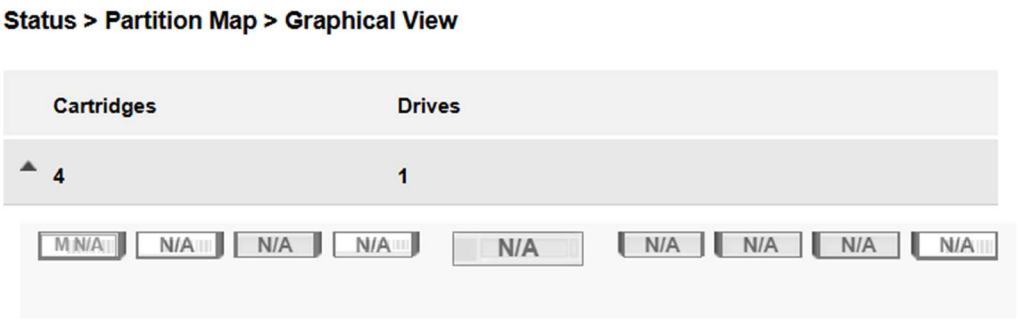
Warning state and error state for a specific drive or cartridge are indicated with icons.



Using Partition Map Graphical View

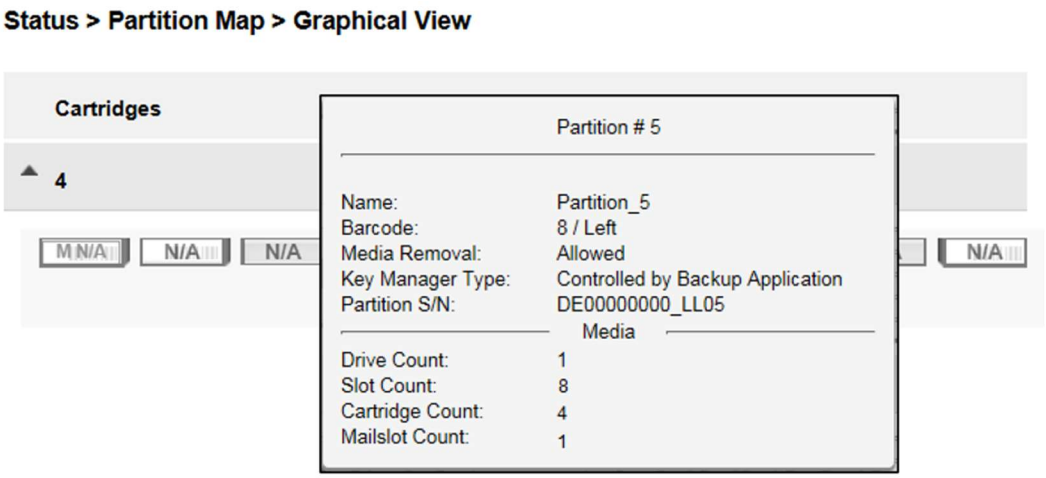
To see the elements organized by logical library or partition, from **Status**, navigate to **Partition Map → Graphical View**.

The graphical view of the partition map displays the partition number for every magazine. Magazine #1, which can be configured as mailslot magazine, displays single slots. When they are configured as mailslots, the slot number gets a leading ‘M’.



Moving the mouse over a partition layer will display additional information:

- **Name** – Partition name
- **Barcode** – Barcode orientation
- **Media Removal** – Indicates whether media removal is allowed or prevented by the host
- **Key Manager Type** – Encryption type
- **Partition S/N** – Serial number of the partition
- **Drive Count** – Number of drives in this partition
- **Slot Count** – Number of slots in this partition
- **Media Count** – Number of cartridges in this partition
- **Mailslot Count** – Number of mailslots in this partition

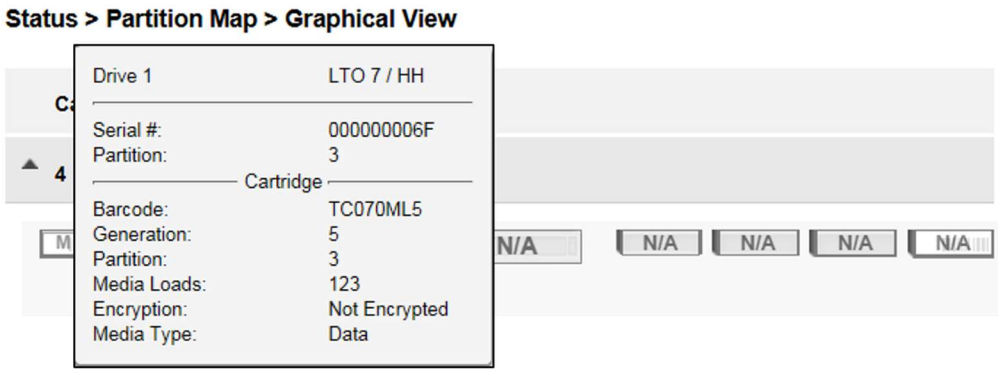


Moving the mouse over a drive will display additional information such as:

- **Drive** – LTO generation of drive and format (Full Height or Half Height)
- **Drive #** - The drive number
- **Serial #** - Serial number of the drive
- **Partition** – The partition number

If a cartridge is loaded in this drive additional information about the cartridge is displayed such as:

- **Barcode** – Barcode data on label
- **Generation** – LTO generation of cartridge
- **Partition** – The partition number
- **Media Loads** – Number of loads
- **Encryption** – Encryption status
- **Media Type** – Data cartridge, Cleaning Cartridge



Using Partition Map Configuration Status

To see the configuration of a partition, the elements and their status, from **Status**, navigate to **Partition Map** → **Configuration Status**.

In the configuration status list, you can see:

- **Partition Number** – The partition number
- **Partition Name** – The partition name
- **Partition S/N** – The partition serial number
- **Number of Drives** – Number of drives in this partition
- **Number of Slots** – Number of slots in this partition
- **Number of Mailslots** – Number of mailslots in this partition
- **Barcode Label Length Rep. to Host** – Barcode length reported to the host
- **Barcode Label Alignment Rep. to Host** – Barcode alignment reported to the host
- **Auto Clean** – Indicates whether automatic cleaning of drives is enabled or disabled
- **Key Manager Type** – Encryption type
- **Active Control Path Drive** – LUN drive for this partition
- **LTO7 Multi-initiator SCSI Conflict Detection** – Indicates whether Multi-initiator Conflict Detection is enabled or disabled

Status > Partition Map > Configuration Status

▼ **Partition Number: 1 Partition Name: Partition_1**

▼ **Partition Number: 2 Partition Name: Partition_2**

▼ **Partition Number: 3 Partition Name: Partition_3**

▲ **Partition Number: 4 Partition Name: Partition_4**

Partition Number:	**4**
Partition Name:	**Partition_4**
Partition S/N:	**DE00000000_LL04**
Number of Drives:	▼ **3**
Number of Slots:	**8**
Number of Mailslots:	**1**
Barcode Label Length Rep. to Host:	**8**
Barcode Label Alignment Rep. to Host:	**Left**
Auto Clean:	**Disabled**
Key Manager Type:	**Controlled by Backup Application**
Active Control Path Drive:	**Drive 1 (LTO7 Fibre)**
LTO7 Multi-initiator SCSI Conflict Detection:	**Disabled**

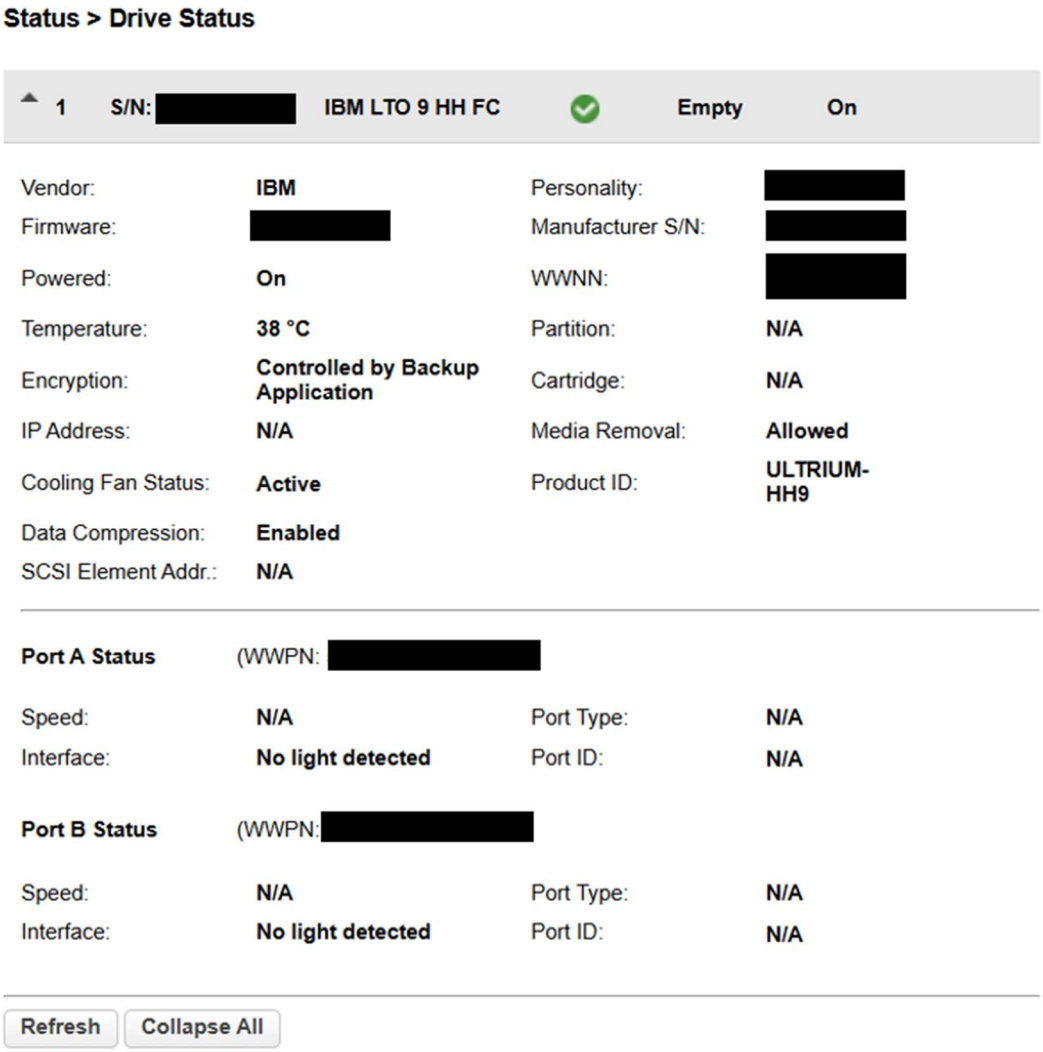
▼ **Partition Number: 5 Partition Name: Partition_5**

▼ **Partition Number: 6 Partition Name: Partition_6**

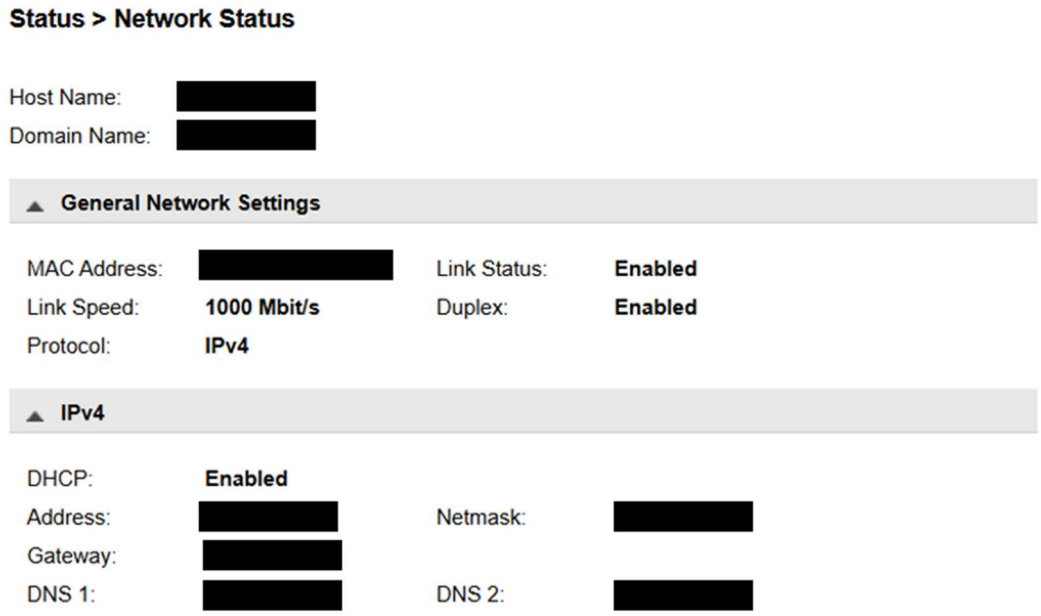
Refresh Expand All

Viewing Drive Status

In the **Status> Drive Status** screen you can see the configuration and status of each drive installed in the library.



Viewing Network Status



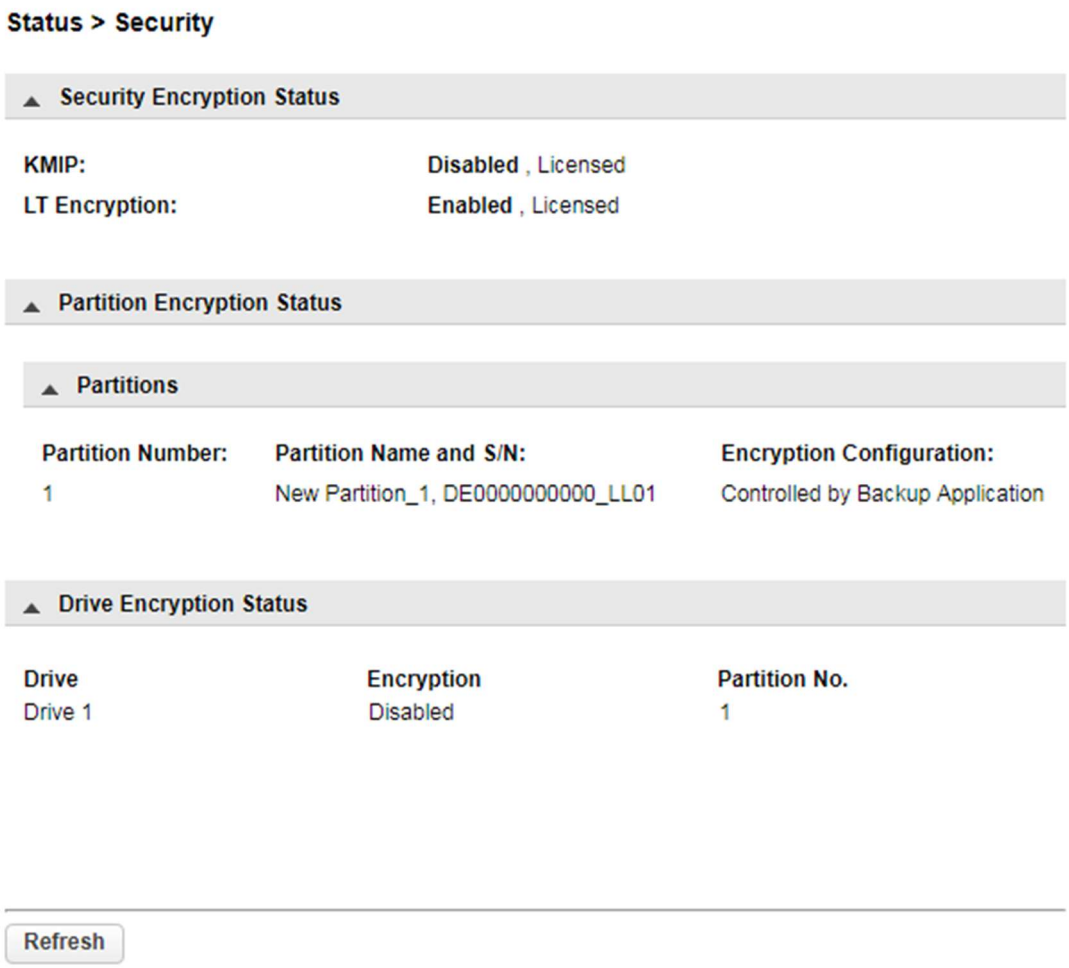
In the Status > Network screen you can see:

- **Host Name** – Library hostname
- **Domain Name**
- **Protocol** – IPV4 or IPv6
- **MAC Address** – A unique identifier for the library controller network interface
- **Link Status** – Enabled or disabled
- **Link Speed** – Speed of the Ethernet connection to the library
- **Duplex** – Enabled or disabled
- IPv4 settings
- **DHCP** – When Enabled, the library requests an IP address from a DHCP server each time the library is powered on.
- **Address** – IP address in use by the library. If DHCP is enabled, this address was obtained from the DHCP server. When DHCP is not enabled, the address was configured.
- **Netmask** – The network mask of the library controller used when DHCP is not enabled.
- **Gateway** – The gateway used when DHCP is not enabled.
- **DNS 1**
- **DNS 2**
- **IPv6 settings**
- **Stateless Addressing** – When Enabled, the device will generate an address for itself based on the routing information obtained from a router advertisement and the MAC address. The device can manage up to five global addresses at the same time, which can be assigned from different routers.

- **Static Addressing** – When Enabled, the library will use a statically-configured address.
- **Static Assigned Address** – The IPv6 address when Static Addressing Enabled is On.

Viewing Security Status

On the **Status > Security** page you can view the encryption status of the library.



Section **Security Encryption Status** provides an overview on the different encryption modes available in the library and their status.

Section **Partition Encryption Status** lists all partitions and its according encryption configuration.

Section **Drive Encryption Status** provides a list with all drives installed in the library and the encryption status for each drive.

Hardware Servicing of the Library



WARNING Only individuals who are informed about the procedures and risks should replace or upgrade this tape drive assembly. Read all troubleshooting documentation and procedures before proceeding with repair or upgrade procedures. Hazardous moving parts exist inside this product. Do not insert tools or any portion of your body into the drive bay openings.



WARNING **Electrical safety -** Disconnect all AC power cords from the library and attached modules before servicing. Allow fans to stop and internal power rails to discharge. Service only field-replaceable units (FRUs). Internal repairs beyond FRUs must be performed by qualified service personnel.



WARNING **Lift / Handling -** Use a **two-person lift**. Do not lift by the bezel, magazines, rails, or rear connectors. Keep the work area **clear of obstructions** and place the unit on a stable, flat surface.



CAUTION **Electrostatic discharge (ESD)**. A discharge of static electricity can damage static-sensitive devices and micro-circuitry. Always use approved **grounding** and **packaging** when handling components.

Before you begin (safe-state checklist)

1) **Stop all jobs** in your backup software; wait until all drives are **idle**.
2) **Eject all cartridges** from drives; close the mailslot.
3) If removing a drive, **power off the drive** in the UI first (Drive Configuration → Power Off).
4) **Shut down** the library (if instructed by the procedure) and **disconnect AC** at the PDUs/outlets.
5) If moving the library, **reinstall the shipping lock** before lifting or transport.

ESD precautions (best practice)

- Transport products in **static-safe containers** (conductive or shielding bags).
- Keep ESD-sensitive parts in their packaging until at a **static-controlled work area**.
- Use a **wrist strap** connected to a **common ground point**; work on an **ESD-dissipative mat**. Ensure tools/equipment are properly grounded.
- Cover the library with **approved static-dissipating material** when open.
- Keep the work area free of **non-conductive** items that hold static (e.g., standard plastic trays, Styrofoam, bubble wrap).
- Avoid touching **pins, leads, or circuitry** directly, handle by edges or brackets.

Possible Tools Needed

- **#2 Phillips Screwdriver** – securing or removing the round-hole rack adapter bracket, securing retention inserts in square-hole rack
- Small Flat Head or **Torx Screwdriver** – retracting the locking screen when moving a library cover, using the magazine manual release
- **T10 Torx Screwdriver** – removing drive bay covers
- **Small Flat Head Screwdriver** – removing a magazine access door
- **Clip Nut Installation Tool** – inserting or removing clip nuts in square-hole racks while installing or removing rack rails

Identifying a Failed Component

Using the RMI:

1) Activate the UID (Unit Identification) LEDs from the **Maintenance** → **UID LED Control** screen on the RMI. This will illuminate the blue LED on the front and rear of the Library to identify the library containing the failed component.
2) Identify the failed component (excluding LTO drives):
3) In the upper left corner of the **Home screen**, locate the module that indicates an error.
4) Click or tap the library for information on the failed component.

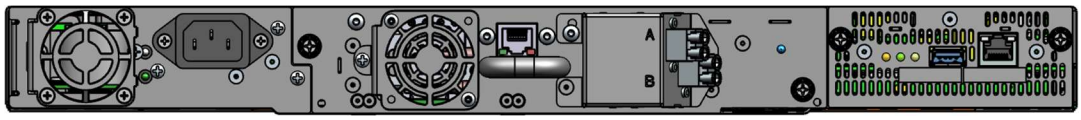
Replacing a Tape Drive

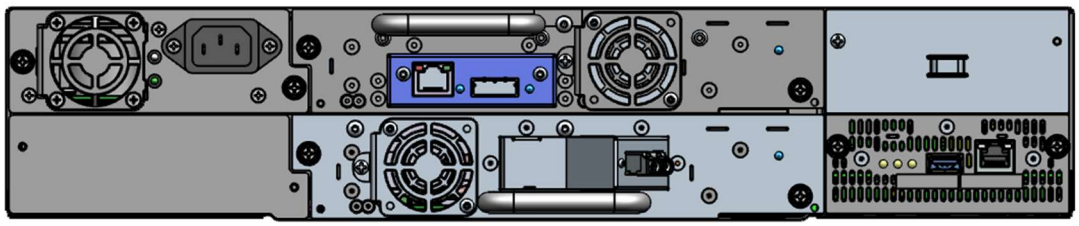
Tape drives are installed at the back of the library. When replacing one drive in a two-drive configuration, you can power down the drive that you are replacing without interrupting power to the rest of the library and the second drive.

Removing a Tape Drive

If you are replacing a tape drive:

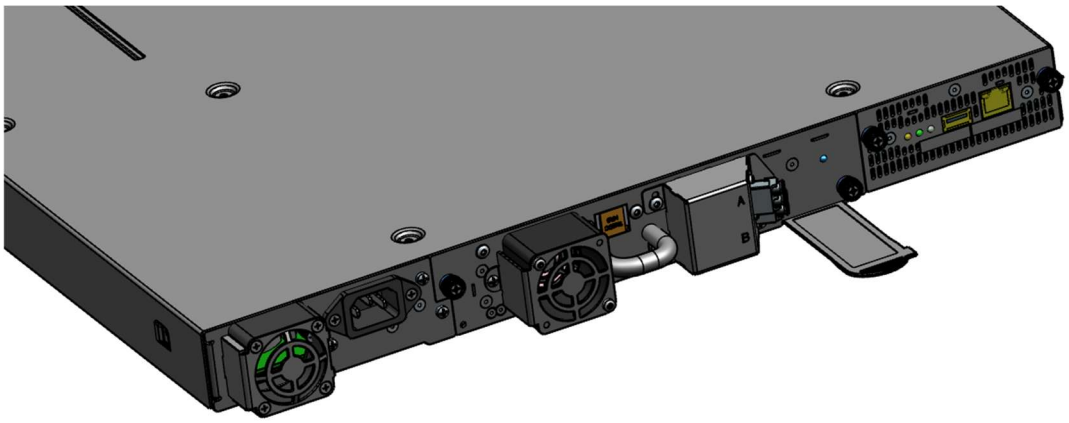
- Make sure the tape cartridge has been removed from the tape drive. Use the operator control panel (OCP) or the remote management interface (RMI) to move the cartridge to a storage slot or mailslot.
- If you are replacing the tape drive in a single drive unit or the master drive in a two-drive unit, verify that backups are not occurring on the drive you are replacing. If backups are occurring on the master drive, verify that the autoloader or library will not be accessed through this drive while the drive is being replaced.
  1) Use the OCP or RMI to power off the tape drive.
  2) Verify that the tape drive assembly LED is off and then remove the FC or SAS cable from the tape drive.

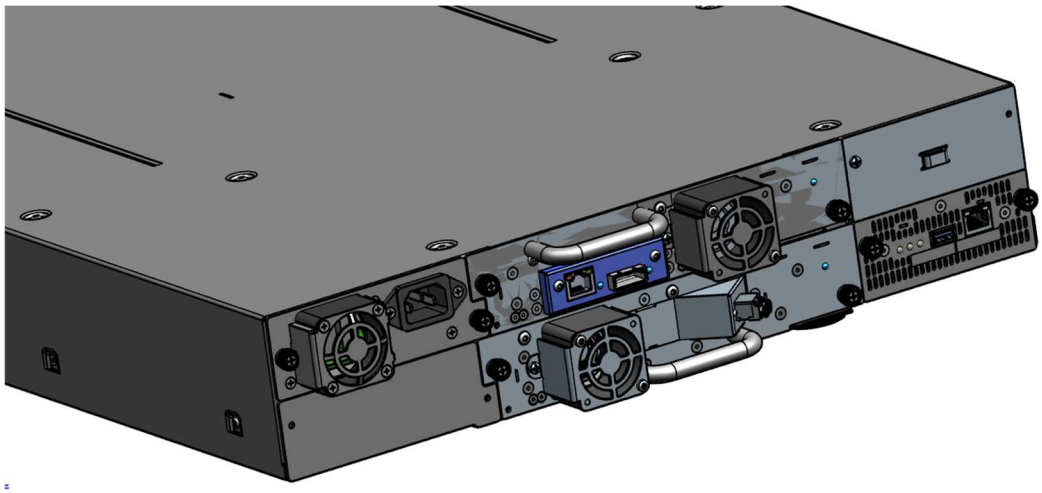




  3) Loosen the blue captive thumbscrews on the tape drive. If there is a lock lever, Press the lock lever to the right and pull straight back on the tape drive handle while supporting the bottom of the drive to remove it from the unit.

! IMPORTANT	Before pulling the **lower** drive sled, **pull the Product ID tag/slide forward** (located below the sled) so it does not snag or get damaged.





	CAUTION	Support the bottom of the tape drive when removing it to avoid damaging any of the internal connections.

Removing a Drive Bay Cover

If you are adding at tape drive:

1) Identify the location for the tape drive. If this is the first tape drive, install it in the bottom drive bay. Otherwise, install the new drive in the next higher drive location.
2) Using a Philips screwdriver, remove one half-height drive bay cover to install one half-height drive.

Installing a Tape Drive

1) Align and slowly insert the new tape drive into the drive bay while supporting the drive assembly. The tape drive should be flush with the back panel of the device.
2) Tighten the captive thumbscrews with your fingers until the tape drive is secure.
3) Reconnect data cable(s). Attach the appropriate SAS/FC cable(s); ensure latches/screws are engaged and strain relieved.

Verifying the Installation

1) Power on the drive from the OCP or RMI, if necessary.
2) Confirm that the library recognizes the new tape drive by checking the OCP or RMI. The new drive should appear in the library status overview area on the left side of the screen.
3) Use the RMI or OCP to verify that the tape drive has the current firmware. Update the firmware if necessary.

Removing and Replacing a XTL Module – Ethernet or Thunderbolt

Removing an XTL Module **interrupts host data access** (iSCSI/Thunderbolt path). Stop all jobs, unmount any mounted volumes, and eject media from all drives **before** proceeding.

To remove a XTL Module

1) **Stop operations**: Ensure all library/drive operations have stopped and no cartridges are loaded. Expect hosts to lose access during the procedure.
2) **Disconnect external cables**
    a. SAS: Label and unplug the SAS cable from the SAS OUT port on the XTL Module.
    b. **Ethernet Module**: Disconnect Data and Management Ethernet cables.
    c. **Thunderbolt Module**: Loosen SymplyLOCK, then disconnect the Thunderbolt cable. Remove SymplyLOCK from the port.
3) **Loosen** the two captive thumbscrews on the module.

!	**IMPORTANT**	Before pulling the **lower** drive sled, **pull the Product ID tag/slide forward** (located below the sled) so it does not snag or get damaged.

4) **Extract the module**: Pull **straight back** on the module handle to slide the sled out. Support the module; **do not rock or twist**.

To replace XTL Module

1) **Inspect the replacement**: Confirm no physical damage; check connectors for bent pins, cracks, or debris.
2) **Align & insert**: Support the module and slide it **straight** into the bay, aligning sled rails with the chassis guides.
3) **Slide fully home**: Gently push the module in until it is **fully seated** and the **captive thumbscrews align** with their holes. Do not rock or twist.
4) **Secure**: Tighten the **captive thumbscrews** evenly until snug.
5) **Reconnect cables**: Attach required cables: **SAS**, **Ethernet (Data/Management)**, and/or **Thunderbolt**. Ensure latches/screws engage and cables are strain-relieved.
    a. For Thunderbolt, fit and tighten **SymplyLOCK** to retain the cable.

6) **Power state**: The XTL Module **auto-powers on** when inserted. Wait for the module and library to report **Ready**.
7) **Verify & configure**
    a. **Thunderbolt Module:** No additional configuration required.
    b. **Ethernet Module:** Log in to the **web UI** with the default credentials and configure **Data port IPs**/network as required. For detailed steps, see the [SymplyPRO Ethernet Appliance User Guide].

Post-install checks (recommended)

- Library shows **Ready**; no faults/alerts on the OCP/RMU.
- Drives are detected and inventories complete.
- Host(s):
    - **iSCSI:** Reconnect targets; verify sessions and present LUNs.
    - **Thunderbolt:** Confirm device enumerates and tape/robotic appear.
    - **SAS (internal link):** Verify drive path is up.
    - **Fibre Chanel (internal link):** Verify drive path is up.
- Backup software rescan: **tape drive(s)** and **medium changer** visible and operational.
- Run a **Wellness Test** or test **load/unload** to confirm robotics.

Moving the Library

When moving a library within the rack, to a different rack, or in a rack to a different physical location, care must be taken to avoid personal injury and damage to the library.

WARNING

WARNING: To reduce the risk of personal injury or damage to equipment:

- Extend the leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install the rack stabilizer kit on the rack.
- Extend only one rack component at a time. Racks might become unstable if more than one component is extended.
- Slide or rail mounted equipment is not to be used as a shelf or a workspace.
- Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed.
- Ensure that you are properly grounded when touching static sensitive components.

WARNING: The autoloader weighs 11.5 kg (25.4 lb) without media and 13.1 kg (28.9 lb) with media (eight cartridges).
When moving the autoloader, to reduce the risk of personal injury or damage to the autoloader:

- Observe local health and safety requirements and guidelines for manual material handling,
- Always remove all tapes to reduce the overall weight of the autoloader, and
- Obtain adequate assistance to lift and stabilize the autoloader during installation or removal.

Risk of damage to devices

When placing a module into or removing the module from a rack:

- Extend the rack's levelling jacks to the floor.
- Ensure that the full weight of the rack rests on the levelling jacks.
- Install stabilizing feet on the rack.
- Extend only one rack component at a time.

To move a library within a rack or into a different rack

1) Save the library configuration.
2) Remove the tape cartridges from the tape drives and magazines and power off the library.
3) Disconnect the power cords and cables and unlock the alignment mechanisms.

	**CAUTION**	Failure to disconnect all cables can result to damage to the cable and/or the mating electronic assembly in the library.

4) Remove other modules from the rack if necessary.
5) Remove the rack rails from the rack.
6) Verify that the destination rack is level side to side and front to back.
7) Install the rack rails in the destination rack.
8) Install the library in the rack.
9) Replace the cables and lock the alignment mechanisms.
10) Connect the power cords, power on the library, and verify the operation.
11) Replace the tape cartridges.

Replacing a Power Supply

The SymplyPRO XTL 8 does not have a customer replaceable power supply. The following procedure applies only to the SymplyPRO XTL 24

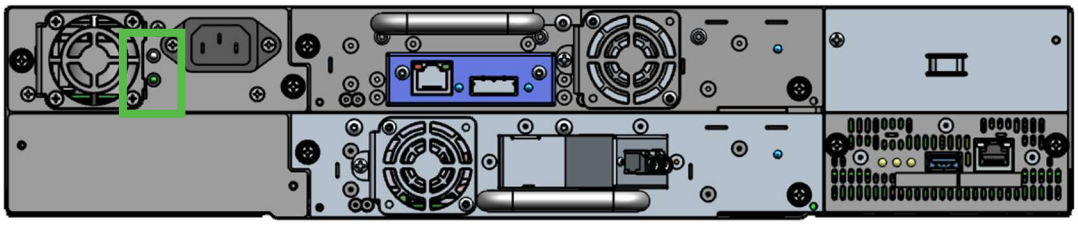
	**CAUTION**	Static Sensitive Risk of damage to devices • A discharge of static electricity damages static-sensitive devices or micro circuitry. • Proper packaging and grounding techniques are necessary precautions to prevent damage.

Identifying the Failed Component

See the OCP or RMI Home screen to identify the failed component. Activate the UID LEDs from the **Maintenance > UID LED Control** screen to locate the library in the data centre. For detailed instructions, see [Identifying a Failed Component].

Preparing to Remove the Power Supply

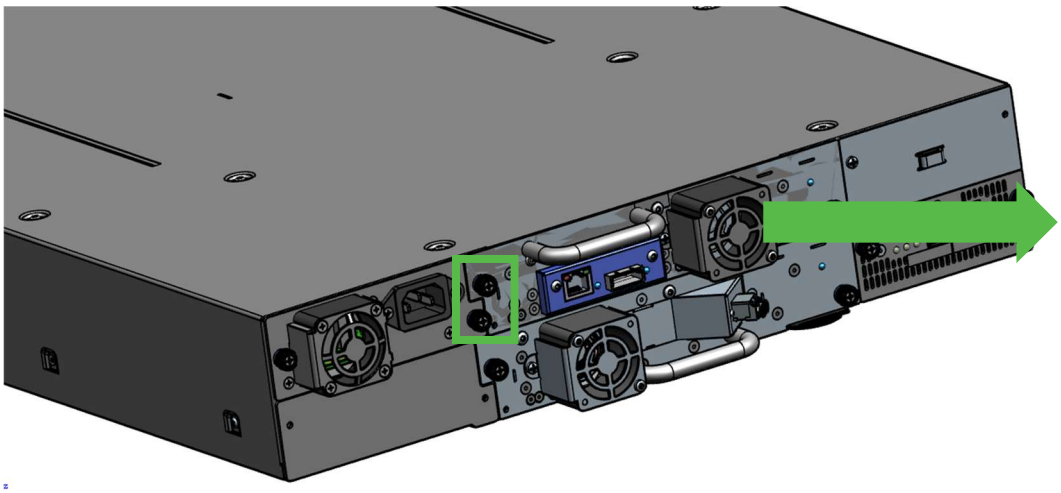
1) Locate the failed power supply on the rear of the library by the LEDs; either the green LED is unlit, or both LEDs will be unlit.



2) Unplug the AC power cord from the power supply you are replacing.

Removing the Power Supplies

1) Loosen the two blue captive thumbscrews with your fingers on the power supply.
2) Using the thumbscrews (one on each side), slowly pull the power supply approximately 10 cm (4 inches) from the back of the library.
3) Use one hand to completely remove the power supply from the library while using the other hand to support the bottom.

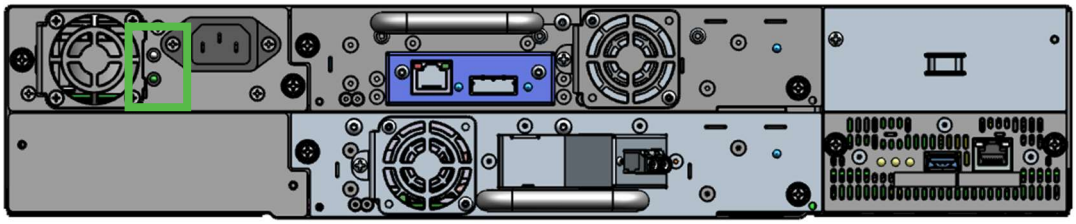


Installing the New Power Supply

1) Position the new power supply onto the alignment rails.
2) Slide the power supply into the module until it is flush with the back panel of the library.
3) Tighten the blue captive thumbscrews with your fingers to secure it to the library.
4) Attach the AC power cord to the new power supply.

Verifying the Power Supply Installation and Operation

1) Verify that the new power supply is operating properly by checking the power supply LEDs:
    a. The white (1) LED should be lit.
    b. The green (2) LED should be lit (if module is on).



Using the OCP or RMI, confirm that the power supply is operating correctly; the event that indicated the power supply was faulty should be cleared.

2) If the UID LEDs are still illuminated, deactivate them using the RMI.

Replacing a Controller Board

Identifying the Failed Component

	CAUTION	• Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed. Ensure you are properly grounded when touching static sensitive components. • You must power off the library to install or replace this part or damage may occur.

!	**Important**	Do not replace both the chassis and the controller with repair components in the same procedure. The firmware will not allow the library to operate if both components are replaced at the same time. The library WWID and serial number are saved in the controller and within the chassis. When one is replaced, the data from the original component is transferred to the repair component. If replacing both the chassis and controller, you must power cycle the library between component replacements.

See the OCP or RMI Home screen to identify the failed component. Activate the UID LEDs from the **Maintenance > UID LED Control** screen on the RMI to locate the library in the data centre. For detailed instructions, see [Identifying a Failed Component].

Saving the Configuration

The library configuration settings are on the library chassis and will be restored automatically when the controller is replaced. However, it is recommended to save the configuration settings before removing the controller board. See [Saving the Library Configuration to a File] for instructions on saving configuration settings to a file or USB flash drive via the OCP or RMI.

Powering Off the Library

Power off the library from the front panel. Depress the power button and hold it for 3 seconds. If the library does not perform a soft shutdown, depress and hold the power button for 10 seconds.

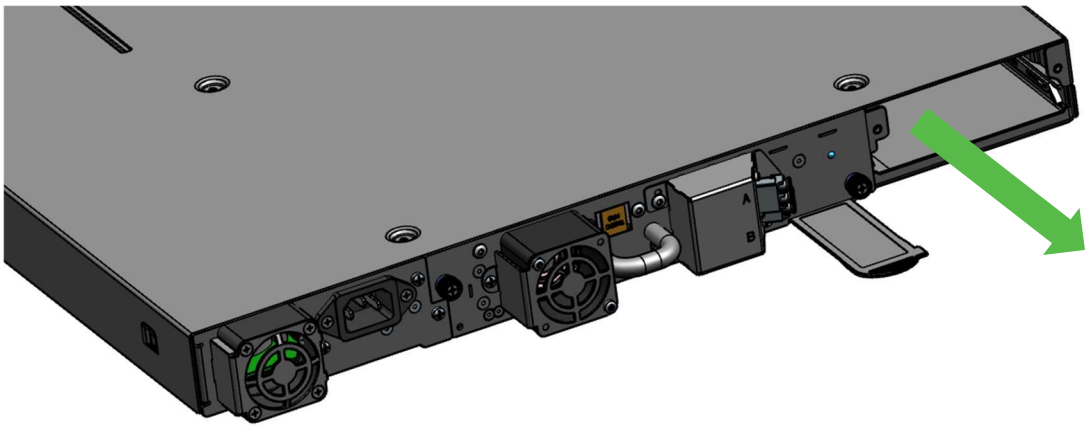
Verify that all host processes are idle.

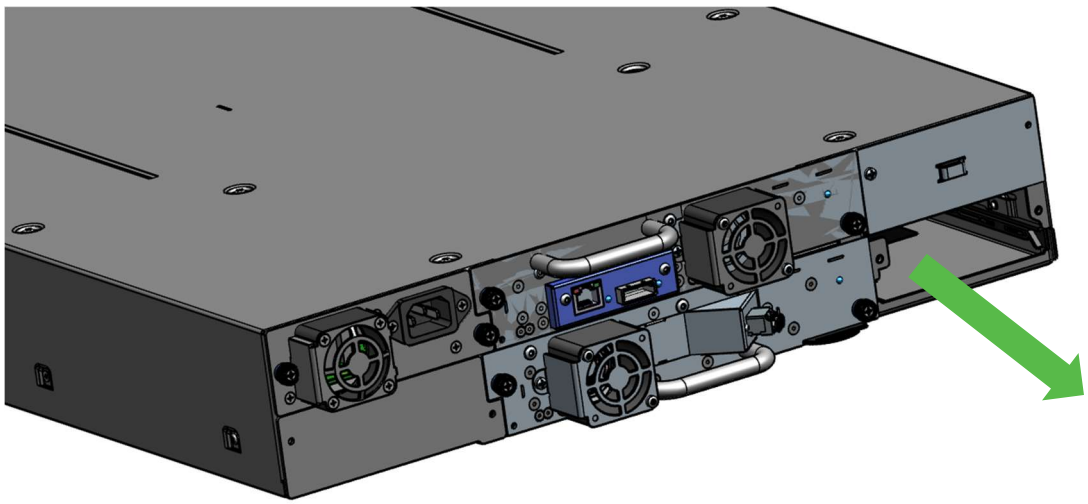
Preparing to Remove the Controller Board

1) Unplug the AC power cables from the library containing the failed controller.
2) On the library containing the failed controller.
3) Remove the Ethernet cables and the USB device.

Removing the Library Controller

1) Loosen the two blue captive thumbscrews on the controller.
2) Using the thumbscrews, slowly remove the controller from the library.





Installing the Library Controller

1) Position the new controller on the alignment rails.
2) Slide the controller slowly into the library until it is flush with the back panel of the library.
3) Tighten the blue captive thumbscrews with your fingers to secure it to the library.
4) Replace the Ethernet cable, and the USB device removed previously.
5) Plug in the AC power cables.

Powering On the Library

Power on the library by pressing the power button on the Library just below the OCP; the green light will illuminate. When the library is powered on, it inventories the tape cartridges in the magazines, checks the firmware version, configures the tape drives.

Verifying the Library Controller Installation

1) Using the OCP or RMI, click or tap **Status > Library Status > Module x** to view the controller status.
2) Using the OCP or RMI, check for events; the event that indicated the controller was faulty should be cleared.
3) Verify that the library has the most up-to-date firmware revision. To find the version of firmware installed on the library, check the upper left corner of the OCP or RMI.



4) If replacing the Library controller, upgrade the firmware if necessary.
5) Update the firmware from the **RMI Maintenance > Firmware Upgrades > System Firmware** screen.
6) If replacing the Library controller, restore the previous settings by restoring them from a file of saved settings, or by entering them using the OCP or RMI.
7) If the UID LEDs are still illuminated, deactivate them using the RMI.
8) Resume the host applications.

Removing and replacing the base chassis

In rare cases Symply may need to replace the SymplyPRO XTL 8 or XTL 24 base chassis, and a replacement will be shipped to you.

WARNING

WARNING: To reduce the risk of personal injury or damage to equipment:

- Extend the levelling jacks to the floor.
- Ensure that the full weight of the rack rests on the levelling jacks.
- Install the rack stabilizer kit on the rack.
- Extend only one rack component at a time. Racks might become unstable if more than one component is extended.
- Slide or rail mounted equipment is not to be used as a shelf or a work space.
- Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed.
- Ensure that you are properly grounded when touching static sensitive components.

WARNING: The autoloader weighs 11.4 kg (25.13 lb) without media and 13.1 kg (28.66 lb) with media (eight cartridges).
When moving the autoloader, to reduce the risk of personal injury or damage to the autoloader:

- Observe local health and safety requirements and guidelines for manual material handling,
- Always remove all tapes to reduce the overall weight of the autoloader, and
- Obtain adequate assistance to lift and stabilize the autoloader during installation or removal.

Risk of damage to devices

When placing a module into or removing the module from a rack:

- Extend the rack's levelling jacks to the floor.
- Ensure that the full weight of the rack rests on the levelling jacks.
- Install stabilizing feet on the rack.
- Extend only one rack component at a time.

Before you begin (safe-state checklist)

1) **Stop all jobs** in your backup software; wait until all drives are **idle**.
2) **Eject all cartridges** from drives; close the mailslot.
3) Label all **data/management cables** to preserve topology.
4) If present, note which bay contains optional modules (Ethernet/Thunderbolt).

ESD precautions (best practice)

- Transport products in **static-safe containers** (conductive or shielding bags).
- Keep ESD-sensitive parts in their packaging until at a **static-controlled work area**.
- Use a **wrist strap** connected to a **common ground point**; work on an **ESD-dissipative mat**. Ensure tools/equipment are properly grounded.
- Cover the library with **approved static-dissipating material** when open.
- Keep the work area free of **non-conductive** items that hold static (e.g., standard plastic trays, Styrofoam, bubble wrap).
- Avoid touching **pins, leads, or circuitry** directly; handle by edges or brackets.

Possible Tools Needed

- **#2 Phillips Screwdriver** – securing or removing the round-hole rack adapter bracket, securing retention inserts in square-hole rack
- Small Flat Head or **Torx Screwdriver** – retracting the locking screen when moving a library cover, using the magazine manual release
- **T10 Torx Screwdriver** – removing drive bay covers
- **Small Flat Head Screwdriver** – removing a magazine access door
- **Clip Nut Installation Tool** – inserting or removing clip nuts in square-hole racks while installing or removing rack rails

Remove the existing chassis from the rack

1) Get adequate assistance to **support** the library during removal/installation.
2) **Remove both magazines**.
3) **Power off** via the front panel, then **disconnect** all power and data/management cables.
4) **Remove drive(s)** and **XTL Ethernet & Thunderbolt modules**
    a. Label and disconnect the cables.
    b. Note the position of the tape drives they must be installed in the same location in the new chassis.
    c. Loosen blue thumbscrews, carefully pull the drive (or module) straight out.
5) **Power supply (PSU):** Loosen the blue thumbscrews, pull the PSU straight out, then install it in the replacement chassis and tighten.
6) **Library controller:** Loosen blue thumbscrews, remove the controller, then install it into the replacement chassis and tighten.
7) From the **front**, loosen the two **captive** screws that secure the mounting brackets to the rack.
8) With assistance, **slide the library out** and place it on a stable surface.

Shipping lock handling:

1) **Replacement chassis (new unit):** The shipping lock is at the **top centre** of the library, secured by a **yellow label**. **Peel off the yellow label** and **remove the lock** before power-on. Store the lock/label in the accessory kit for future transport.
2) **Old chassis (return unit): Reinstall its shipping lock** before packing for return. If already removed, retrieve it from the accessory kit and fit it per the label instructions.

Install the replacement chassis in the rack

1) With assistance, **slide the replacement chassis** onto the rails already mounted in the rack.
2) Tighten the **front bracket captive screws** to anchor the chassis.
3) **Transfer field-replaceable units (FRUs) to the replacement chassis**
    a. **Tape drive(s):** Install into the replacement chassis. Tighten thumbscrews.
    b. **XTL Module(s) (Ethernet/Thunderbolt, if fitted):** Install into the replacement chassis. Tighten thumbscrews.
    c. **Power supply (PSU):** Install into the replacement chassis. Tighten thumbscrews
    d. **Library controller:** Install into the replacement chassis. Tighten thumbscrews

5) **Reconnect cables:**
    a. AC mains (to properly earthed outlets/PDUs; separate circuits if dual PSUs).
    b. Host/data (SAS/FC/Thunderbolt/iSCSI) and **management Ethernet**.
6) **Reinsert both magazines**.
7) **Power on** the library.
8) Run the **Wellness Test.**

Return the old chassis:

1) **Securely repack** the replaced chassis with its **shipping lock installed**.
2) Include any required RMA documentation and return to **Symply** per instructions.

Library Troubleshooting

CAUTION	This library is designed to operate **only** when installed in a rack using the supplied rail kit. Operating it off-rail (e.g., on a table, bench, or rack shelf) can cause alignment and robotics errors. Do **not** place any weight on top of the library—the top cover is not load-bearing and doing so may lead to faults or damage.

Installation problems – Troubleshooting

Most installation issues trace to **SAS/FC/iSCSI/Thunderbolt connectivity**, **host adapter settings (multi-LUN)**, **drivers**, or **backup-software configuration**. If the application can't communicate with the library, work through the checks below.

Quick checks (in order)

- **Power/Ready:** Library fully **initialized** (inventory complete) and no OCP faults.
- **Cabling:** Correct **connector type** (SFF-8644/8088/FC), firmly latched, no adapters out of spec, shortest practical cable.
- **Multi-LUN:** Host/HBA must scan **LUN 0 = tape drive**, **LUN 1 = medium changer**. If only the drive appears, enable **Report LUNs / multi-LUN** on the HBA/initiator and rescan.
- **Drivers:** Correct **tape drive** driver (vendor or Microsoft) and **Medium Changer** driver (typically **Unknown Medium Changer** on Windows).
- **Software rescans:** Restart/Rescan devices in your backup/archive application after OS sees both drive **and** changer.
- **Partitions:** If you changed partitions, **rescan** in the OS and software.

Compatibility

- Verify the library/drive generation and interface are **supported** by your **HBA/NIC/Thunderbolt** stack and your **data-protection application**.
- Check HBA/NIC **firmware + driver** levels recommended by the vendor.

Host adapter installation

- Confirm the HBA/NIC is **properly seated** and detected by the OS; correct driver loaded; no device errors.
- Disable **MPIO**/multipathing for **tape/changer** devices (not supported/necessary).
- For SAS HBAs, do not use RAID adapters. Make sure HBA supports TLR.

Data-protection application

- Some suites need an **extra module/license** to control **library robotics**. Install/enable it.
- Ensure the app is set to use **OS drivers** (or its own) consistently—avoid double-installing conflicting drivers.
- After hardware changes, **restart application services** and rescan hardware.

Interface-specific checks

SAS

- **Cables:** Verify all SAS connectors are fully seated at **both ends**. If a mini-SAS plug won't insert, check the **keying**—the drive uses the **standard end-device key (location 4)**. A differently keyed cable will not fit and likely won't work.
- **Length/integrity:** Keep to vendor limits (**typically ≤ 5 m or 16.4 ft**) and avoid adapters/converters between HBA and library. Replace questionable cables.
- **Connector condition:** Inspect for damage/debris; clean or replace as needed.
- **HBA support/firmware:** Use a **qualified SAS HBA** (not a RAID controller), supported by the host OS and the library, with **current firmware/drivers**.

Thunderbolt

- Point-to-point only.
- Verify the **Thunderbolt cable is approved.** Use **SymplyLOCK** for strain relief.
- **Authorized** (Windows: Thunderbolt Control Centre).
- Ensure **driver has permission to run in macOS.**

Fibre Channel (FC)

- **Speed:** Set link speed to **Automatic** (recommended). If you know the HBA/switch speed, select it explicitly; otherwise use Auto.
- **Port type:** Ensure the correct **port type** is selected (**Fabric/Point-to-Point** vs **Loop**). Loop requires extra configuration; if unsure, set **Auto**.
- If the screen shows **No Link**, (Speed Status "–" and the drive's rear **Link LED is off**):
  - The **speed** is likely incorrect—set to **Automatic**.
  - If issues persist, set **port type** to **Auto Detect**.
- If no connection light is shown on the drive:
  - The **cable may not be seated**. Check it is fully inserted into **Port A** on the tape drive.
  - The **cable may be damaged**. FC cables are delicate; if bent/twisted sharply, replace with a known-good cable.

iSCSI (XTL Ethernet Module)

- In **iSCSI Initiator**: add the portal (module IP), **Connect** targets, make sessions **persistent**.
- No MPIO for tape. Ensure CHAP/ACLs allow access.
- Keep **MTU** consistent end-to-end for jumbo frames.
- Confirm data and management IPs are correct and reachable.
- Ensure Data Ports are separate subnets.

OS visibility tests

If tape drive(s) and/or medium changer are visible to the OS **Common symptoms → likely causes**

- **Drive visible, library is not visible:** Multi-LUN disabled; incorrect zoning/LUN masking; iSCSI session only exposing LUN 0.
- **Software sees library but no barcodes:** Barcode **length/alignment** not matching app expectations; inventory required.
- **Access denied/busy:** Stale **reservations/locks** in application; stop services and clear reservations.
- **Intermittent I/O errors:** Over-length/poor cables; tight bend radius; mixed link speeds; power/grounding issues.

Before contacting support (collect)

- OCP **Service → Wellness Test** result and any on-screen error codes.
- RMU **support bundle/logs** (if available).
- OS details: lsscsi/mtx output (Linux) or **Device Manager** screenshots/PowerShell output (Windows).
- HBA/NIC **model, firmware, driver** versions; switch/zoning screenshots (FC) or iSCSI session details.
- Backup application **version** and device scan report.

Performance troubleshooting

Backups touch many components—from the source disks and file system, through the backup server and software, to the tape library. Throughput is limited by the **slowest** element in that chain. Identify the bottleneck, then tune or upgrade it.

Common bottlenecks to review:

- Average file size.
- File system / storage layout.
- Connection from the backup/archive host server to the disks.
- Backup/archive server resources.
- Backup/archive software and method.
- Connection from the host to the library.
- Media (type, condition, environment).

Average File Size

Disks must **seek** to each file before reading. Lots of small files increase seek time and reduce throughput. Calculate average file size: **total data size ÷ number of files**. If the average is **≤ ~64 KB**, consider a **sequential/image/block** backup that captures a whole volume/LUN rather than file-by-file (trade-off: restores may be whole-image or slower for single files).



NOTE File fragmentation will also cause excessive drive seeking, which lowers performance, so ensure that files are regularly defragmented.

File storage system

How data is organised on disk matters. Spreading I/O across multiple disks (e.g., with RAID) lets some disks **seek** while others **read**, improving throughput. Single, non-RAID disks are slowest; high-end arrays are fastest. Converting standalone disks to a suitable RAID level can help.

Connection from the host to disk storage

The host-to-storage link must sustain the tape drive's **streaming rate**. Insufficient bandwidth starves the drive. Use interfaces and link speeds that match your workload; on lower-speed Ethernet–based storage, consider **multiple connections** (properly configured/teamed per vendor guidance).

Backup/archive Server

Ensure enough **CPU** and **RAM** to move data while the backup software and other services run. Monitor during jobs; if resources are saturated, add CPU/RAM or reduce concurrent tasks.

Backup/archive software and method

Each backup method has its own impact on performance, depending on how well it can keep data streaming to the tape drive. In most cases, native applications don't have the features required to maximize performance for LTO tape drives. It is recommended to use a full-featured backup or archive application with this library.

File-by-file backup or archive methods provide the best restore performance if you only need to restore individual files. However, if the average file size is small, file-by-file methods will significantly reduce performance.

Disk image, flash, or sequential backup methods provide the fastest performance because they back up an entire disk, partition, or LUN, which minimizes disk seeking. The disadvantage is that backup and restore operations work on an entire disk, partition, or LUN. You might not be able to back up a subset of files or restore a single file. If you can restore a single file, the restore process will be slow.

Database backup performance will vary based on the model. To improve performance when backing up data from a database:

- Use specific backup agents for the database.
- Use the latest versions of the databases.
- Do not back up individual mailboxes.
- Do not back up specific records or do a record-by-record backup.
- Do not back up when the database is in heavy use.

Connection from the host to the library

Interfaces used with modern LTO drives are rarely the bottleneck, but **bad cables**, **excess length**, or **mismatched settings** can be. Keep within **recommended cable lengths**, use quality, like-for-like cables, and verify link settings (speed/port type/MTU as applicable).

Media

Media type and condition affect performance. For best results, use media that matches the drive generation, retire worn or damaged cartridges, and clean drives when prompted. **LTO-9 and LTO-10** have **tighter environmental tolerances** than earlier generations; operating **outside**—or consistently **near the edge**—of the recommended temperature and humidity ranges can **significantly degrade throughput** and increase error recovery (stop–start streaming). Keep conditions stable and in specifications and allow cartridges to acclimatise before use.

Operation Problems

Power Problems

Problem	Solution
Device does not power on.	1. Check all power cord connections. 2. Check the LEDs on the power supplies. 3. Make sure the power button on the front panel has been pressed, and the green **Ready** LED is lit. 4. Make sure the outlet has power. Try another working outlet. 5. Replace the power cord.
No message appears on the OCP display.	1. Check all power cord connections. 2. Check the LEDs on the power supplies. 3. Make sure the power button on the front panel has been pressed, and the green **Ready** LED is lit. 4. Make sure the outlet has power. Try another working outlet.

Failure/Attention Indications Displayed on the Front Panel

Problem	Solution
The LCD displays a warning or error icon.	Tap the icon to see more information about the event on the LCD.
The LCD displays an error code.	Look up the error code, try to resolve the failure, and power cycle the library (see **Event Codes**).

Tape Movement Problems

Problem	Solution
Tape stuck in drive.	Try the following steps, in this order, to remove the stuck tape. **NOTE:** The tape drive must rewind the tape before ejecting it. This can take as long as five minutes, depending on how much tape must be rewound. Once the tape is rewound, the eject cycle will take fewer than 16 seconds. The **Ready** light flashes while the tape rewinds. Wait for the tape to finish rewinding before attempting another operation. 1. Attempt to unload the tape from your backup software. 2. Shut down the backup software and stop the operating system's removable storage services. From the **Operation > Move Media** screen, attempt to unload or move the tape to a slot. 3. Power down the library, disconnect the cable from the drive, power up the library, and wait until the tape drive is idle or ready. From the **Operation > Move Media** screen, attempt to unload or move the tape to a slot. 4. From the **Operation > Force Drive Media Eject** screen, attempt a force eject or emergency unload operation. **IMPORTANT:** Inspect the tape cartridge that was stuck. Damage or misplaced labels on the cartridge could have caused the load/unload failure. Discard any tape cartridge found to have issues.
Tape cannot be removed from storage slot	If the OCP or RMI is still operational: 1. Unlock the magazine from the **Operation > Open**

Problem	Solution
	Magazine screen and extend it to access the storage slot. 5. Grasp the cartridge and remove it from the storage slot. Some tapes need to be inserted and removed several times to condition them for free movement in and out of the magazine. 6. Check the barcode label and verity that it is secure to the cartridge. 7. Check the cartridge for damage. 8. Check the storage slot for damage.

Media Problems

Problem	Solution
Cleaning or data cartridge incompatible with drive.	1. Check the event log to see which cartridge is incompatible. 2. Make sure you are using data and cleaning cartridges that are compatible with the drive and model of your device and that you are using the correct cartridge type for the operation. The device automatically unloads incompatible cartridges, the **Attention** LED flashes. Export the media.
Cannot write to or read from tape.	1. Make sure that the cartridge is not a WORM cartridge that has already been used. 2. Make sure that the cartridge is write enabled (move the write-protect switch to the enabled position). 3. Make sure the data cartridge is compatible with the drive model. LTO tape drives can read data cartridges from two generations back and write to data cartridges one generation back. 4. Make sure you are using an Ultrium cartridge that has not been degaussed. **Do not degauss Ultrium cartridges!** 5. Make sure that the cartridge has not been exposed to harsh environmental or electrical conditions and is not physically damaged in any way. 6. Many backup applications do not read or write to cartridges that were created using a different backup application. In this case, you may have to perform an erase, format, or label operation on the cartridge. 7. Make sure you understand any data protection or overwrite protection schemes that your backup application may be using, which could prevent you from writing to a given cartridge.

Problem	Solution
	8. Retry the operation with a different, known good tape. 9. Clean the tape drive from the **Operation > Clean Drive** screen.

Attention LED is Lit

Problem	Solution
Both the Attention and Cleaning LEDs are lit.	This is most likely caused by a dirty drive that cannot read a tape and marks the tape invalid. Log into the OCP or RMI and check the event log to see which drive has reported that it needs cleaning. Clean the drive with an approved Ultrium cleaning cartridge.
A particular cartridge sets off the cleaning light.	Remove the cartridge from the library.
A cartridge recently imported from a different environment is causing issues.	Media that is moved from one environment to another can cause issues until it has acclimated to the new conditions. A cartridge should be acclimated for at least 24 hours before being used, particularly if it has been stored at a substantially different temperature or level of humidity than the device.
The Attention LED is lit but the Cleaning LED is not lit after a cartridge load.	1. The library was unable to complete the requested operation with the selected tape cartridge. 2. Use only cartridges that are compatible with the drive type 3. Use the correct type of cartridges for the operation. For example, use a cleaning cartridge for cleaning. 4. Make sure you are using an Universal cleaning cartridge
The Cleaning LED is lit after using a cleaning cartridge.	The cleaning cartridge has expired. A cleaning cartridge will expire after 50 cleaning cycles.
A particular cartridge sets off the Attention LED and possibly the Cleaning LED.	1. Retry the operation with a different cleaning cartridge. 2. If the Attention LED is cleared and the drive has been cleaned, and then immediately re-displays each time a particular cartridge is reloaded, that cartridge should be suspected as being defective. 3. If this occurs, export the cartridge and load a known good cartridge. In some cases, a cartridge can be worn out, have a defective Cartridge

Problem	Solution
	4. Memory, or have been formatted as a Firmware Upgrade Cartridge. 5. Any cartridge that is suspected of being defective or contaminated should NOT be reused in any drive. 6. If the bad cartridge is a cleaning cartridge, it might be expired.

Inventory Problems

Problem	Solution
The library displays incorrect bar codes.	1. Verify that the label is properly applied. 2. Verify that the label is not soiled.

RMI Network Connection Issues

Problem	Solution
Cannot connect to the RMI.	1. Verify that the Ethernet cable is connected to the library's controller board and to the LAN. 2. Verify that the link LED on the RJ45 (LAN) connector is lit when the device is powered up. If the LED is not lit, the device is not communicating with the LAN. See your network administrator for help. 3. Verify that the device has been configured with a valid static network address or DHCP has been enabled so the device can obtain a network address. If using DHCP, write down the device's network address from the OCP login screen. If the device did not obtain a valid address via DHCP, verify that the DHCP server is up and the library has network access to it. If necessary, set a static network address instead. 4. Enter the library's IP address into the address bar of a web browser connected to the same LAN as the device. If the RMI web page does not display, ping the device's IP address. If the ping fails, verify that the device has a valid network address and that there are no firewalls or other obstructions to network traffic between the computer with the web browser and the device. See your network administrator for help.

Cleaning Problems

Problem	Solution
Cannot load the cleaning cartridge.	1. Make sure you are using an Ultrium cleaning cartridge. 2. Make sure the cleaning cartridge has not expired. A cleaning cartridge will expire after 50 cleaning cycles. 3. Power cycle the library.

Finding Event Information

You can find error codes by viewing log files from the **Maintenance > Logs and Traces > View Logs** screen or downloading support tickets from the **Maintenance > Download Support Ticket** screen. See [Viewing Log Files] or [Downloading Support Tickets].

Unlocking the Magazine

It is recommended that you unlock the magazine using the unlock buttons or RMI. If these methods fail, or if a magazine needs to be removed when the power to the device is off, you can release the magazine manually. Only one magazine can be open at a time.

NOTE As a best practice, perform this procedure while applications are idle. While the magazine is extended, the library robotic assembly cannot move media

Using the Magazine Unlock Button

1) Press the button for more than 3 seconds. This will start the unlock operation for the magazine, indicated by the LED slowly flashing.
2) When the magazine is unlocked the LED starts quickly flashing
3) Pull out the magazine from the library. As soons as the magazine is pulled out, the LED switches OFF.

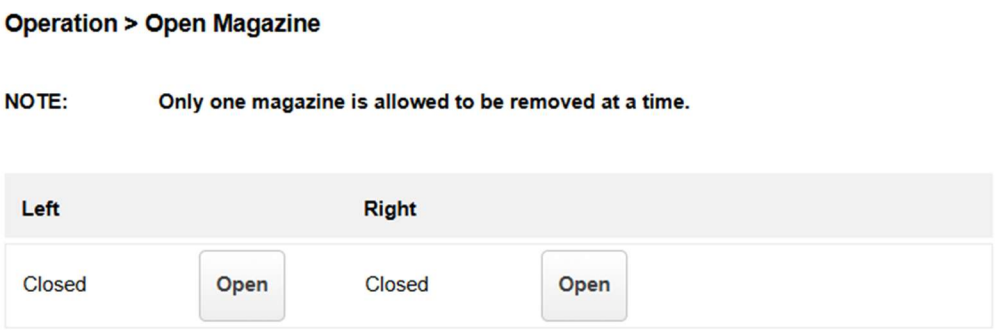
NOTE

- Opening a magazine will take the library off-line.
- The magazines will relock after 30 seconds.

IMPORTANT Wait before pulling out the magazine until the LED is quickly flashing and OCP message says that the magazine is unlocked

Using the RMI to Unlock Magazines

1) Log in as an administrator.
2) On the Home screen, click **Open Magazine**.
3) Click **Open** in the left or right magazine column within the module containing the magazine to be opened.



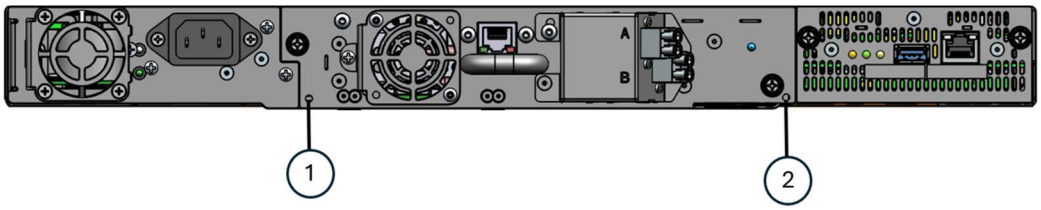
1) A message box indicates when the magazine has been unlocked.
2) Open Magazine screen shows that the magazine is now unlocked.

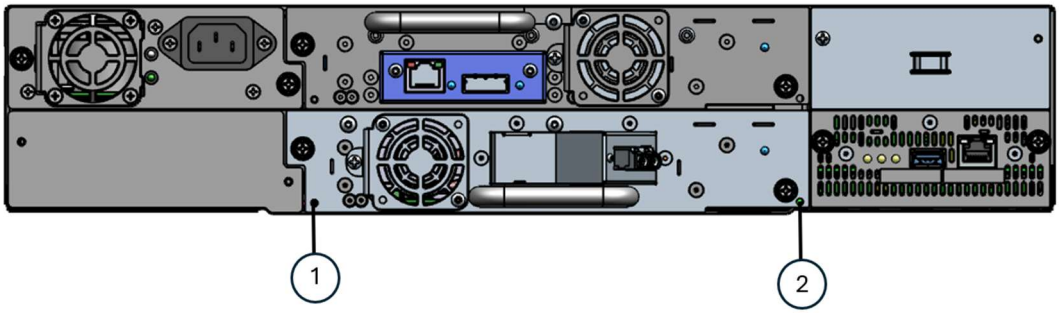
	NOTE	If not removed, the magazines and the mailslot will relock after 30 seconds.

Using the Manual Release to Unlock Magazines

To manually release the magazine, insert a small flat head screwdriver or Torx driver into the appropriate magazine release hole and gently push the tab in.

!	**IMPORTANT**	Do not exert force once you encounter resistance. Doing so can damage the device.





Item	Description
1	Release hole for right magazine
2	Release hole for left magazine

Unloading a Stuck Tape

If the tape is stuck in a tape drive, eject the tape from the drive from the **Operation > Force Drive Media Eject** screen.

If a tape is stuck in a magazine, open the magazine, grasp the cartridge, and pull it out of the storage slot.

Running Library Tests

The library provides tests to verify library operations.

- **Wellness Test** – exercises a general health check on the library functionality by running the following partial tests:
  - Basic Hardware Review
  - Robotics Initialization Test
  - Barcode Scanning Test
  - Move Media Test
- **System Test** – exercises overall library functionality by moving cartridges within the library. Cartridges are returned to their original location. See [System Test].
- **Slot to Slot Test** – randomly exchanges cartridges within the library. Cartridges are NOT returned to their original locations. See [Slot to Slot Test].
- **Element to Element Test** – moves a cartridge to a specific element and then returns it to its original location. See [Element to Element Test].
- **Robotics Test** – exercises all robotic assembly movements and sensors. See [Robotics Test].

Acronyms and Abbreviations

Item	Description
FC	Fibre Channel
FH	Full Height
GUI	Graphical User Interface
HBA	Host Bus Adapter
HH	Half Height
LUN	Logical Unit Number
OCP	Operator Control Panel
RMI	Remote Management Interface
SAN	Storage Area Network
SAS	Serial Attached SCSI
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
UID	Unit Identification
USB	Universal Serial Bus
WORM	Write Once, Read Many
WWPN	World-Wide Port Name

Event Codes

Error Events

Event Code	Message Text and Description	Details and Solution
2000	Failed to move cartridge.	Verify the source and destination elements and retry the move operation.
2003	The library's temperature has exceeded the critical limit.	Check to ensure 1) the chassis fan is functioning in each module present, 2) the drive cover plates are installed where no drive exists, 3) all power supplies are installed, 4) the ambient room temperature is within limits.
2004	Library Startup Failure.	Verify that magazines are closed, cartridges are fully seated, and that there are no robotic assembly obstructions. Verify all modules are powered and any expansion modules are cabled correctly with the inter module cable. Verify there is a top and bottom cover properly installed on the library. Also, verify the module alignment locks (at rear of module) are in the proper position. If the robot moves front to back, but not vertically, the robot shipping lock could be positioned incorrectly and should be moved to either the fully locked or fully unlocked position. If the error persists, review library events for more information and/or reboot the library.
2009	Library test failed due to robotics assembly problem.	Review test requirements and retry the test, if the test continues to fail check for robotic obstructions or other robotic problems. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library,

Event Code	Message Text and Description	Details and Solution
		first power off the library by pressing the front power button for 5 seconds and select the Default Park location. Once the library is powered off, remove the left magazine of the lowest library module, and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.
2021	Database access error.	Restore a configuration backup and perform a power cycle.
2022	Drive has been hot removed while in active status as LUN master.	Reinsert the removed drive at the same position as it was removed.
2023	Internal software error.	Check for a new system software version for upgrade.
2024	Exception thrown by application not handled.	Check for a new system software version for upgrade.
2027	Move failed pulling cartridge from slot.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the slot or drive. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library, first power off the library by pressing the front power button for 5 seconds and select the Default Park location. Once the library is powered off, remove the left magazine of the lowest library module, and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the

Event Code	Message Text and Description	Details and Solution
		magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.
2028	Move failed inserting cartridge to slot.	Check for labels or cartridge misalignments that would prevent the cartridge from moving into the slot or drive. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library, first power off the library by pressing the front power button for 5 seconds and select the Default Park location. Once the library is powered off, remove the left magazine of the lowest library module, and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.
2029	Initialization failure due to robot front to back positioning error.	Check for obstructions in the pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. Check if robotics assembly stuck in lock mechanism, move robotics assembly apart from lock mechanism and enable lock mechanism correctly.
2032	Initialization failure due to robot rotation positioning error.	Check for obstructions in the vertical pathway of the robot such as a cartridge sitting in the shuttle of the robot or any other impedance to robotic movement.
2033	Initialization failure due to robot vertical positioning error.	Check for obstructions in the vertical pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or

Event Code	Message Text and Description	Details and Solution
		on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library, first power off the library by pressing the front power button for 5 seconds and select the Default Park location. Once the library is powered off, remove the left magazine of the lowest library module, and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.
2035	Initialization failure due to robot gripper positioning error.	Check for obstructions in the vertical pathway of the robot such as a cartridge sitting in the shuttle of the robot or any other impedance to robotic movement.
2037	Robotics firmware version upgrade failed.	Reboot or power cycle system.
2038	Lost connection to Module.	Ensure that all modules are powered and have the interconnect cable properly attached. Reboot or power cycle the system.
2039	Cartridge left in robot gripper, unable to be moved to any open location.	Enable Mailslots and ensure that some of them are free. Then power cycle library. If still failing, open covers and remove cartridge manually from gripper.
2040	Wellness test failed with critical error.	
2045	Wellness test failed because move media test failed.	The minimum requirements for the Wellness are at least one unloaded drive and one data cartridge compatible with that unloaded drive installed in the library. If no drives are unloaded or no compatible media is found, the test will fail and an error event will be generated. To view event details from RMI, click on the event, and then view all of the event details to see what elements

Event Code	Message Text and Description	Details and Solution
		were involved in the move failure. Additionally, check for obstructions in the pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. Check if robotics assembly stuck in lock mechanism, move robotics assembly apart from lock mechanism and enable lock mechanism correctly.
2046	Wellness test failed because drive communication test failed.	Remove and reseat the drive canister to ensure that the drive is fully seated. If the issue persists then reset the drive. Use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).
2047	Wellness test failed because the barcode scanning test failed.	Verify that there is no obstruction in front of the barcode scanning module on the cartridge table located on the robotics assembly. If the error persists replace the robotics assembly. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library, first power off the library by pressing the front power button for 5 seconds and select the Default Park location. Once the library is powered off, remove the left magazine of the lowest library module, and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.
2051	Wellness test failed because of the failing robotic test.	Check for obstructions in the pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment.

Event Code	Message Text and Description	Details and Solution
		Check if robotics assembly stuck in lock mechanism, move robotics assembly apart from lock mechanism and enable lock mechanism correctly. Ensure that the spooling cable is fully seated in the Base Module and connected correctly to the robotic assembly.
2052	An open magazine was detected in one or more modules and as a result the system was taken offline.	Ensure that all magazines are completely inserted and properly locked. Do not open magazines using the emergency release while the library is operating and the robot is moving.
2056	Initialization failure due to picker push pull positioning error.	Check for obstructions in the horizontal pathway of the robotics assembly such as a cartridge sticking out or a cable impeding progress.
2061	Move failed pulling cartridge from drive.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the drive.
2062	Move failed inserting cartridge to drive.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the drive.
2063	Move failed positioning picker in front of drive.	Check for obstructions in the vertical or horizontal pathway of the robotic assembly. Examples could include a cartridge that is not seated completely in a slot, a robotics assembly is not sitting horizontally level, or a problem with the robotic spooling cable that is impeding progress.
2064	Library test failed with critical error.	
2065	Library startup process failed because of robotics initialization issue.	
2066	Library startup process failed during inventory scan.	

Event Code	Message Text and Description	Details and Solution
2067	For safety reason the robot movement was halted in place.	Ensure that all magazines, top or bottom covers and unit locks are completely inserted and properly locked. Do not open magazines using the emergency release or remove covers or unit locks while the library is operating and the robot is moving. Ensure that all modules are powered and have the interconnect cable properly attached.
2069	Initialization failure due to barcode reader error.	
2070	Inventory scan failed because of Elevator axis problem.	Check for obstructions in the vertical pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library, first power off the library by pressing the front power button for 5 seconds and select the Default Park location. Once the library is powered off, remove the left magazine of the lowest library module, and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.
2071	Cartridge on picker when trying to scan.	Verify that there is no obstruction in front of the barcode scanning module on the cartridge table located on the robotics assembly. If the error persists replace the robotics assembly.
2074	The library startup failed due to a GPIO error.	Reboot or power cycle system.

Event Code	Message Text and Description	Details and Solution
2075	The library startup failed due to an error when trying to open the robotics serial port.	Reboot or power cycle system.
2076	I2C bus signals invalid.	Remove all drive canisters of the affected chassis and reboot the library. If the problem persists, replace the chassis. If not, add one drive after the other until the problem comes back. Replace the last drive added before it failed again.
2079	Could not upgrade barcode reader firmware.	Reboot the library and if the error persists replace the robotics.
2080	Cartridge lost while inserting it into slot/drive.	Check the source/destination element and ensure that there are no obstructions in the pathway of the robot.
2082	Drive with FIPS Secure Mode enabled has been hot removed	Tape drives with FIPS Secure Mode enabled need to be disabled (powered-off) before removing them from the Library. In case of hot removal this event will be created if the drive was active LUN master. A similar event is defined with lower severity (warning) if the drive wasn't LUN master. Reinsert the removed drive at the same position as it was removed. FIPS Secured Mode is enabled on the removed drive. To un-enroll the drive, the drive must be powered down by command or FIPS Secure mode needs to be disabled prior removing the drive.
2087	Error accessing the backplane flash memory.	Reboot the library and if the error persists replace the chassis. Prior to replacing the chassis, ensure you remove all of your tape cartridges. If magazines need to be removed to get access to the tape cartridges, first power down the device and then manually release each magazine. Only one magazine should ever be opened at a time.

Event Code	Message Text and Description	Details and Solution
2092	Locking the Robotics Assembly has failed during Power Down	
2093	Communication to Robotic Controller could not be established	Reboot the library and if the error persists replace the robotics assembly.
2094	An emergency stop condition was detected in one or more modules and prevented the robotic from running the inventory scan	Ensure that all magazines, top or bottom covers and unit locks are completely inserted and properly locked. Please insert all open magazines and install all necessary covers and unit locks before powering on the library. Ensure that all modules are powered and have the interconnection cable properly attached.
2095	Inventory scan failed because of robotic positioning problem	Check for obstructions in the horizontal pathway of the robot such as a cartridge sticking out or lying on the robotics table.
2096	Initializing a communication interface on the library controller failed	Reboot the library and if the error persists replace the library controller
2097	Mechanical re-initialization in context of Robotics error recovery has failed	Reboot the library and if the error persists replace the robotics.
2100	Position to element command failed because of robotics problem	Check for obstructions in the pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. Check if robotics assembly stuck in lock mechanism, move robotics assembly apart from lock mechanism and enable lock mechanism correctly.
2105	Accessor initialization failed due to horizontal positioning problem	Check for obstructions in the horizontal pathway of the accessor such as a cartridge sticking out or lying on the accessors table. The accessor shipping lock might be positioned incorrectly and must be moved to either the fully locked or fully unlocked position.

Event Code	Message Text and Description	Details and Solution
2106	An elevator block was detected and as a result the system was taken offline	Check for obstructions in the vertical pathway of the robot such as a cartridge sticking out. Verify the library's alignment. For proper operation the robot must be able to reach the very bottom of the library. Verify there are no obstructions at the bottom of the library or on the bottom cover of the library in the path of the robot. To check for obstructions at the bottom of the library, first power off the library by pressing the front power button for 5 seconds. Once the library is powered off, remove the left magazine and verify the entire area of the bottom cover is free of any objects that might obstruct the robot's path. After clearing any obstructions, replace the magazine, power the library on, and after the library finishes initialization and inventory, verify no further critical events were generated.

Warning Events

Event Code	Message Text and Description	Details and Solution
4000	A reported drive canister fan speed is too slow.	Ensure there are no obstructions in the fan
4002	A drive sent a clean request.	Clean the drive with an approved cleaning cartridge.
4003	The drive configuration failed.	Remove and reseat the drive canister and retry the operation. If the drive installed is a different generation than the drive previously installed, you may need to reset defaults and reconfigure the drive as appropriate. Use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).

Event Code	Message Text and Description	Details and Solution
4004	The drive status request failed.	Remove and reseat the drive canister to ensure that the drive is fully seated. If the issue persists then reset the drive. Use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).
4005	Drive is reporting a critical TapeAlert.	Power-cycle the drive and verify whether the drive reports the same TapeAlert. Use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).
4006	A drive temperature reported is above the threshold.	Verify the drive fan is spinning, is not obstructed and that the ambient temperature is within specification. Also, ensure that there are drive bay cover plates in place in each location where there is no drive installed. The drive cover plates are required for proper airflow.
4007	Cartridge error.	Remove the cartridge and inspect it for damage. Retry operation with another cartridge.
4008	Cleaning tape expired.	Discard the cleaning cartridge and retry the cleaning operation with a new cleaning cartridge.
4010	Drive is not compatible with this library.	Remove the incompatible drive. Only install drives that are supported by the library.
4012	Move Cartridge operation failed due to drive or media issue.	View the event details to determine which cartridge was involved. Verify surrounding events pointing to problems with this media in other move operations. Remove the media from the Library and physically inspect the media to ensure there is no physical damage. If the media appears to be undamaged, put the media back into the library and retry the move operation. If the problem persists retry the operation

Event Code	Message Text and Description	Details and Solution
		with a different cartridge in the same drive. If the problem follows the media, remove the media from use. If the problem follows the drive, use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).
4014	Library test failed due to a drive issue.	Verify the test parameters and retry the test. If the test fails, check the library event log for specific events associated with this drive. Use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).
4016	Backup configuration data to base module failed.	Attempt to save a library configuration, power cycle the library and retry the operation.
4017	Restore configuration data from Chassis failed.	Attempt to save a library configuration, power cycle the library and retry the operation.
4018	Firmware upgrade failed, tape drive reported an error applying the firmware file.	Verify that the firmware file is correct for the drive(s), ensure the drive(s) is/are in a healthy state with no cartridge in the drive, then retry the operation.
4019	General Drive Firmware bundle upgrade failure.	Verify that the firmware file is correct for the drive(s), ensure the drive is in a healthy state with no cartridge in the drive, then retry the operation.
4020	Database has been reset due to a problem that prevented the library from powering up.	If the library was restored to default settings, restore a saved configuration by using a previously saved config file. If not, config file exists, then proceed in configuring the library. If the library was restored to default settings, restore a saved configuration by using a previously saved config file. If not, config file exists, then proceed in configuring the library.

Event Code	Message Text and Description	Details and Solution
4021	Drive has been hot removed while in active status as data transfer device.	
4025	Library test failed due to a cartridge error.	Remove the cartridge and inspect it for damage. Retry operation with another cartridge.
4028	Drive cannot use this media due to it being an unknown or unsupported format. Possibly the media is the wrong generation of media.	Check LTO generation for media and drives. Remove cartridges which are not compatible to your tape drives.
4029	Incompatible media move operation blocked by media barcode ID check.	Check if Media barcode label is matching LTO generation. Replace label or remove incompatible media from your system.
4030	Move cartridge operation failed due to media error.	Remove the cartridge and inspect it for damage. Retry operation with another cartridge.
4037	Loss of redundant data path	Data path failover for tape drives needs both primary ports connected. Please verify your cabling.
4038	Drive configuration failed	Advanced data path failover is enabled for a drive which doesn't support this feature. Disable advanced path failover for this drive or replace it with a drive supporting this feature. If this event occurred after replacing a drive, first remove the drive from the partition, then run the expert partition wizard again, and add the new drive back into the partition.
4039	Drive configuration failed	Advanced control path failover is enabled for a drive which doesn't support this feature. Disable advanced path failover for this drive or replace it with a drive supporting this feature. If this event occurred after replacing a drive, first remove the drive from the partition, then run the expert

Event Code	Message Text and Description	Details and Solution
		partition wizard again, and add the new drive back into the partition.
4040	Advanced Data Path Failover	Check cabling and all network components between the affected drive and host computer
4043	Control path failover occurred	The active control path switched from active path to the failover path in context of advanced path failover. Check cabling and all network components between the affected drive and host computer
4044	One of the Library tests failed because of a source element or destination element is currently not accessible.	One of the Library tests failed because of a source element or destination element is currently not accessible
4046	Drive configuration failed because of missing DPF License	Basic or advanced data path failover is enabled but feature is not licensed. Disable path failover or install appropriate license for the configured feature (data path or control path failover).
4047	Drive configuration failed because of missing CPF License	Basic or advanced control path failover is enabled but feature is not licensed. Disable path failover or install appropriate license for the configured feature (data path or control path failover).
4051	Encryption Kit key generation - media was loaded	A tape drive with enabled encryption was loaded during manual MSL Encryption Kit key generation
4052	Encryption Kit key generation - media was loaded	A tape drive with enabled encryption was loaded during manual MSL Encryption Kit key generation
4059	Drive configuration failed because it does not support encryption	A Drive which is not supporting encryption became included to an encrypting partition and is now offline after configuration error.

Event Code	Message Text and Description	Details and Solution
		Replace Drive by a model of LTO generation 4 or higher or disable encryption for this partition.
4060	Connection to the KMIP server failed.	Verify username and password as well as all needed SSL certificates needed for connecting to the KMIP server. Verify that the KMIP server is reachable within the network.
4061	Key not found on KMIP server.	Verify that the requested key is available on the KMIP server. Check the KMIP server logs for additional details.
4062	Key creation on KMIP server failed.	Check the KMIP server logs for additional details about why key creation failed.
4063	KMIP configuration invalid.	Use the KMIP configuration wizard to verify the KMIP configuration.
4064	KMIP feature not licensed.	Disable KMIP or install appropriate license for KMIP feature.
4065	A tape alert flag was reported by a drive.	
4066	Automatic control path failover failed because disabling LUN drive failed	The automatic process for switching control path from active to passive drive in case of disabling LUN master drive failed.
4067	Cleaning cartridge will soon be expired and should be replaced.	Replace the cartridge.
4069	Configuring the drive default map ID was not possible	Ensure the drive is powered up, is communicating with the library, and has up to date firmware. If this error persists, disable Secure Manager for the entire library and re-enable it.
4072	No cleaning cartridge in partition available for auto cleaning.	Auto cleaning is enabled, but the partition contains no labelled cleaning cartridge. The library was unable to perform the auto clean function for one or more drives in this partition. Install a valid and labelled cleaning cartridge into the partition and then perform a load and unload on the

Event Code	Message Text and Description	Details and Solution
		drive that needs cleaned to initiate the auto cleaning.
4073	Medium source element empty.	Check the source slot visually and rescan inventory. Additionally check for valid and readable barcode label.
4074	Medium source element empty.	Check the source slot visually and rescan inventory. Additionally check for valid and readable barcode label.
4075	Cartridge lost while extracting it from slot/drive.	Check the source/destination element and ensure that there are no obstructions in the pathway of the robot.
4076	Secure Manager feature not licensed	Disable Secure Manager or install appropriate license for Secure Manager feature
4077	Unlocking the right magazine failed.	Reboot the library and retry the operation. If the error persists replace the chassis. If the magazine needs to be removed to get access to the tape cartridges, first power down the device and then release the magazine manually. Only one magazine can be open at a time.
4078	Unlocking the left magazine failed.	Reboot the library and retry the operation. If the error persists replace the chassis. If the magazine needs to be removed to get access to the tape cartridges, first power down the device and then release the magazine manually. Only one magazine can be open at a time.
4079	Unlocking the mailslot failed.	Reboot the library and retry the operation. If the error persists replace the chassis. If the mailslot needs to be removed to get access to the tape cartridges, first power down the device and then release the entire magazine manually. Only one magazine can be open at a time.
4080	Wellness test failed with warning.	

Event Code	Message Text and Description	Details and Solution
4081	Library test failed with warning	
4084	Failed reading logged in hosts table	Ensure the drive is powered up, is communicating with the library, and has up to date firmware. If this error persists, disable Secure Manager for the entire library and re-enable it.
4085	Too many retries of drive command needed because of Unit Attention or Not Ready condition.	
4086	Move operation failed due to the inability accessing the database.	Ensure the network the library is connected to is operating normally and ensure the library is running the latest firmware. Library needs reboot.
4087	Key Server Token is over 90% full	
4093	Could not obtain an IP address from DHCP server.	Check the network configuration settings and check if the DHCP server is reachable. Use the network configuration menu or unplug the network cable and plug it in after a few seconds to trigger an automatic reconfiguration of the network interface.
4094	Drive interface I/O error.	Reboot the library for new initialization of hardware and device drivers. Get in touch with service if the problem persists.
4095	Library test failed. Not enough valid cartridges available for testing.	
4099	An unexpected reset of robotics has been detected.	Ensure that the spooling cable is fully seated in the Base Module and connected correctly to the robotic assembly. If the error re-occurs replace the robotic assembly.
4100	Drive with FIPS Secure Mode enabled has been hot removed	FIPS Secured Mode is enabled on the removed drive. To un-enroll the drive, the drive must be powered down by command

Event Code	Message Text and Description	Details and Solution
		or FIPS Secure mode needs to be disabled prior removing the drive.
4101	Drive Configuration failed because FIPS Secure Mode is not supported	Replace drive by a model of LTO generation 6 or higher or disable FIPS Secure Mode for this partition. If a drive with LTO generation 6 or higher is already in use, then upgrade to the latest drive firmware version.
4102	Drive Configuration failed due to a FIPS Secure Mode operation error	Retry the operation. If the error persists, verify the drive firmware is up to date and the partition FIPS support mode settings are correct
4103	Drive Configuration failed during disabling FIPS secure mode	This drive was probably enrolled on a different library. Check the "CN" value on the drive status page showing the serial number of the library where the drive was enrolled. Put the drive back to that library and un-enroll first before moving the drive to a different library. See the user guide for more information.
4105	Drive Configuration failed during enabling FIPS secure mode	This drive was probably enrolled on a different library. Check the "CN" value on the drive status page showing the serial number of the library where the drive was enrolled. Put the drive back to that library and un-enroll first before moving the drive to a different library. See the user guide for more information.
4106	Drive Configuration failed during enabling FIPS secure mode	Please re-run the FIPS secure mode wizard to generate certificates or disable FIPS secure mode. See the user guide for more information.
4108	Drive secure mode hard enabled	To correct this configuration mismatch, either enable FIPS Support Mode for the specified partition or install the FIPS Secure Mode-disabled firmware variant on the drive. Note: The drive is online and functional, encryption keys will continue to be provided in the correct encrypted format, and the drive status reports FIPS Secure Mode enabled.

Event Code	Message Text and Description	Details and Solution
4109	Drive in the partition is running FIPS Secure Mode-disabled firmware	To correct this configuration mismatch, either disable FIPS Support Mode for the specified partition or install the FIPS Secure Mode-enabled firmware variant on the drive. Note: The drive primary ports are offline, and the drive status reports FIPS not supported.
4111	Drive firmware upgrade failed because the specified image is not FIPS Secure Mode enabled	This event indicates that the drive's partition has FIPS Support Mode enabled, and that prior to loading this firmware image the partition must first have FIPS Support Mode disabled. Use the LTO FIPS Support Mode wizard to disable FIPS Support Mode on the partition containing this drive. Verify that the firmware file is correct for the drive(s), ensure the drive(s) is/are in a healthy state with no cartridge in the drive, then retry the operation.
4112	Move Cartridge failed due to cartridge not seating properly	Verify surrounding events for drive problems. Retry the operation with the same source and destination combination, if the problem persists retry the operation with a different cartridge in the same drive. If the problem follows the media, the media should be check for physical damage and no longer used. Use the library RMI to pull a drive support ticket and check the device analysis section for more help (HPE Library and Tape Tools must be installed to view support ticket).
4113	Move Cartridge operation failed due to cartridge not properly taken over from Drive.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the slot or drive.
4115	Internal software error	Check for a new system software version for upgrade
4120	No empty drive available for system test.	
4121	No compatible media available for system test.	

Event Code	Message Text and Description	Details and Solution
4122	No cartridge available for slot to slot test.	
4123	No empty slot available for slot to slot test.	
4124	Drive or media statistics could not be retrieved when unloading the tape.	Check for additional warning tickets. Replace media if media related tape alert flags reported.
4125	Multi-Initiator conflict warning Event	Multiple SCSI command initiators were detected on a drive, in a partition that has multi-initiator conflict detection enabled (LTO7 or newer feature). View the list of host WWNN addresses listed in this event and take action to prevent host access for any host WWNN you do not want accessing the tape drive. Once all of the other host WWNNs are prevented from accessing the tape drive, close the event and continue normal use of the tape drive
4127	Drive re-configuration caused by sled reset	
4129	Media removal prevented by drive.	Check backup application how to allow media removal from drive. If unsuccessful, try Force Drive Media Eject option in operations menu.
4130	Wellness test failed because drive not finally initialized.	Wait until drive initialization completed and run test again.
4138	USB overcurrent detected	Make sure the USB device is correctly inserted and that it does not consume more current than specified in manual.
4140	Personality mismatch detected	Replace either chassis or library controller to ensure that all parts in the stack are matching the personality of the main library controller.
4141	Drive requires cleaning	Clean the drive with an approved cleaning cartridge.
4143	Magazine removed for extended period	Please note that the library is offline when a magazine is removed. Please reinstall

Event Code	Message Text and Description	Details and Solution
		the magazine to get the library online again.
4145	Key not available on MSL Encryption Kit token	Verify that the MSL Encryption Kit token containing the requested key is inserted and logged in.
4146	LTO7 formatted cartridge with a Type M barcode detected.	Replace cartridge barcode label by correct version.
4147	Type M cartridge without a Type M barcode detected.	Replace cartridge barcode label by correct version.
4151	Download of drive firmware image completed, but firmware revision did not change after reboot.	Check if the uploaded firmware image is matching your drive type and generation. Ensure that the image file is not corrupted. Download a new image from the drive vendor's web site if you are not sure about file integrity.
4152	KMIP connection refused - The selected port on the tar get machineis not open, the connection is refused.	Please check that the server application is running on the target machine and the firewall is not blocking the selected port. Get in contact with your IT Personnel to verify the port settings.
4153	KMIP Server does not trust the client certificate - The authentication on server side fails because the client certificate cannot be trusted	Please use a client certificate, which is signed by a trusted Certification Authority (CA) or manually select the untrusted certificate on server side and trust it (not available on all servers).
4154	KMIP Ping to server failed - The target machine couldn't be reached, no network connection possible.	Please verify the that the IP address in the settings is correct. Check that the target machine is powered and connected to the network. Please check the network cable. Verify that the Firewall setting on the target machine allowing ping requests and responses.
4155	KMIP No route to host - The target machine couldn't be reached, the network route	Please check your IP settings (IP Address, Gateway and Netmask) and verify them with your IT personnel. Check that the

Event Code	Message Text and Description	Details and Solution
	to the machine is not available.	Firewall settings on the target machine are correct.
4156	KMIP Handshake failure - The TLS connection couldn't be established because of Handshake errors during certificate exchange.	Check the certificates on server and client side for valid entries and that they are still valid and not expire. Verify that TLS1.2 is enabled on the server. Check the client and server date/time for current time. Ask your IT personnel for new and valid certificates.
4157	KMIP Certificate unknown - The server certificate is unknown, because its root certificate is missing or not trusted.	Run a new certificate request with your server or certificate authority and import the resulting certificate chain.
4158	KMIP Host name lookup failed - The host name on the network couldn't be found. It doesn't exist or is misspelled.	Please verify the entered host name to be correct. Check your DNS address in the network settings. In any case contact your IT personnel for the verification of the entered data.
4159	KMIP certificate verify failed - The TLS server certificate couldn't be verified as a valid and trusted certificate.	Check if your server root certificate has changed. Create a new certificate request against your server to generate a new client certificate based on the changed server certificates.
4163	Drive sled discovery timeout	Ensure that the network is not experiencing broadcast storms or ot her abnormal activity. Reboot or power cyc le the system for re-initialization.
4164	Inventory has been updated due to an unexpected empty or full slot	
4174	KMIP CA certificate failure	Check if you provided the correct CA certificate or the CA certificate on the encryption server has changed.
4176	Failed to send CVTL ticket	Please check whether the configuration of CVTL is correct
4193	Autocleaning has failed	Move a cleaning cartridge per move command into the drive where autoclean

Event Code	Message Text and Description	Details and Solution
		has failed. If the cleaning process fails again, check tape alert flags or events for further failure analysis

Configuration Change Events

Event Code	Message Text and Description
8000	The configuration of a drive changed.
8001	The drive was added or removed from the system.
8002	A partition was added/removed or changed.
8003	A mailslot bank was enabled / disabled.
8004	Drive firmware changed due to firmware upgrade.
8005	The configuration of hostname/domain name has changed.
8006	The email configuration settings have been changed.
8007	The configuration of a date/time format changed.
8009	The timezone configuration has changed.
8011	The network settings have changed.
8013	The NTP time synchronization configuration has changed.
8014	The SSH access was enabled/disabled.
8015	Level of media generation checking has changed.
8016	Library reset default settings invoked by user.
8017	Library FW changed.
8018	The Unlabeled Media Support configuration has changed.
8019	Robotics firmware version upgraded.
8020	A new key was created automatically
8021	Secure manager status changed
8024	Mailslot / Magazine access control configuration changed.
8026	Robotics change detected.
8029	The SNMP configuration changed.
8030	A SNMP target has been added.
8031	A SNMP target has been deleted.
8032	The SNMPv3 settings changed.
8033	The OCP module has been changed.

Event Code	Message Text and Description
8034	A drive reboot has been requested by RMI command or REST interface. This process could cause side effects if done in parallel to running operations.
8040	LDAP Server has been added.
8041	LDAP Server has been modified.
8042	LDAP Server has been deleted.
8043	LDAP User has been added.
8044	LDAP User has been modified.
8045	LDAP User has been deleted.
8046	Logout prevention configuration changed.
8047	FIPS Secure Mode configuration changed
8056	Command View TL configuration changed
8057	New hardware component added to the Library.
8058	Hardware component removed from the Library.
8059	Hardware component of Library replaced.
8062	Auto calibration successfully finished
8064	Password rules configuration changed
8065	User has been added
8066	User has been deleted
8067	Persistent reservations removed
8068	Remote Logging configuration changed
8069	User password has been changed
8070	Default encryption mode for new partitions has been changed
8071	The administrator permission for configuring encryption has been changed
8103	Two-factor authentication has been enabled for user
8104	Two-factor authentication has been enabled for user

Informational Events

Event Code	Message Text and Description
9000	A tape alert flag was reported by a drive.
9001	A drive is present in the system but powered off.
9002	The library was powered on.
9003	Move Medium command was executed.
9004	Inventory scan was performed.
9005	The library was powered down from Front Panel.
9006	The network interface was switched on.
9007	The network interface switched off.
9008	The System Time was synchronized with a NTP server.
9009	A magazine was unlocked and opened.
9010	A magazine was closed and locked.
9011	A mailslot bank was unlocked and opened.
9012	A mailslot bank was closed and locked.
9015	A user logged in at the OCP interface.
9016	A user logged out at the OCP interface.
9017	Encryption Kit password changed
9018	Encryption Kit key request
9019	Encryption Kit key has been created
9020	Encryption Kit password set
9021	Encryption Kit Token has been initialized
9022	MSL Encryption Kit backup
9023	Encryption Kit restore
9024	Drive support ticket created.
9025	Library test started.
9026	Library test successfully finished.

Event Code	Message Text and Description
9027	Library test stopped by user.
9028	Configuration backup to Base Module was successful.
9029	Configuration restore from Base Module was successful.
9031	Library health Status changed to “Status OK”.
9032	Library health status changed to status "Warning".
9033	Library health status changed to status “Critical”.
9038	The library was rebooted through user interface.
9039	Token key creation attempt failed due to media being loaded in one or more drive
9040	Control path switched over from active to passive drive
9041	Key on KMIP server created.
9043	Drive cleaning.
9047	Encryption Kit backup has been initiated
9048	Encryption Kit restore has been initiated
9049	Encryption Kit partial backup has been initiated
9050	More than 5 invalid MSL Encryption Kit PIN attempts
9051	Encryption Kit contains keys that have not been backed up
9052	Encryption Kit is full. Adding or generating new keys prohibited
9053	Encryption Kit key provided
9055	Encryption Kit not present
9056	Encryption Kit was inserted
9057	Encryption Kit was removed
9060	One or multiple configured DNS servers are not responding.
9061	A user account has been locked due to too many invalid login attempts on RMI.
9062	Invalid password used for login
9063	The network port used to contact the encryption server has been changed.

Event Code	Message Text and Description
9064	Backup of certificate created
9065	Certificate has been restored.
9067	LTO7 formatted cartridge with a Type M barcode detected
9068	Type M cartridge without a Type M barcode detected
9071	Encryption Kit password set automatically
9078	Unexpected drive reset occurred
9079	Media initialization needed
9085	A user was logged out of the RMI interface due to a timeout
9086	A user has been logged out of the RMI interface by another user
9087	A user was logged out of the OCP interface due to a timeout
9088	A user has been logged out of the OCP interface by another user

Warranty Information

The SymplyPRO XTL system comes with a limited three (3) year warranty, but with the option to purchase an upgrade to a five (5) year warranty.

Warranty and technical support service can be accessed at www.support.gosymply.com

SYMPLY (“the Company”) warrants its products will be free from defects in material and workmanship for three years from the date of purchase of the product.

This Limited Warranty only applies to the original purchaser of the product and is not transferable to subsequent owners.

This Limited Warranty is void if the product is subjected to abuse, misuse, abnormal, excessive or improper conditions (including, without limitation, attempts to utilize the product under any condition that exceeds its design capabilities, or any other use beyond the use specified in any product instructions), or if the product is altered or modified in any manner. This Limited Warranty does not cover damage to the product due to external causes (including, without limitation, accident, liquids, chemicals, oxidation, corrosion, or exposure to the elements), or problems caused by use of parts and components not supplied by the Company.

The sole remedy under this Limited Warranty is product repair, replacement, or refund of the purchase price, at the sole discretion of the Company. In order to make a claim the purchaser must ship the product to the Company at the purchaser’s expense, together with proof of purchase and a description of the nature of the defect. The Company will not be held responsible for any product that is damaged or lost in transit to the Company.

PURCHASER AGREES THAT SYMPLY SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, SECONDARY OR CONSEQUENTIAL DAMAGES, OR FOR THE DAMAGE, INJURY, OR LOSS OF LIFE, PROPERTY OR OTHER PRODUCTS THE PURCHASER CONNECTS TO THE PRODUCT, OR LOSS OF REVENUE OR DATA, WHETHER BASED ON CONTRACT, TORT, PRODUCTS LIABILITY OR ANY OTHER LEGAL THEORY, EVEN IF THE DAMAGE, INJURY OR LOSS IS CAUSED BY THE NEGLIGENCE OR OTHER FAULT OF SYMPLY. THE FOREGOING WARRANTY IS THE ONLY WARRANTY MADE BY SYMPLY, AND SYMPLY MAKES NO OTHER WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This Limited Warranty shall be governed by the laws of England and the parties hereby submit to the exclusive jurisdiction of the English courts for that purpose. If any provision is declared void or unenforceable by a court of competent jurisdiction with respect to particular circumstances, such provision shall remain in full force and effect in all other circumstances. If any provision is declared entirely void or unenforceable by a court of competent jurisdiction all other provisions of these Terms and Conditions shall remain in full force and effect.